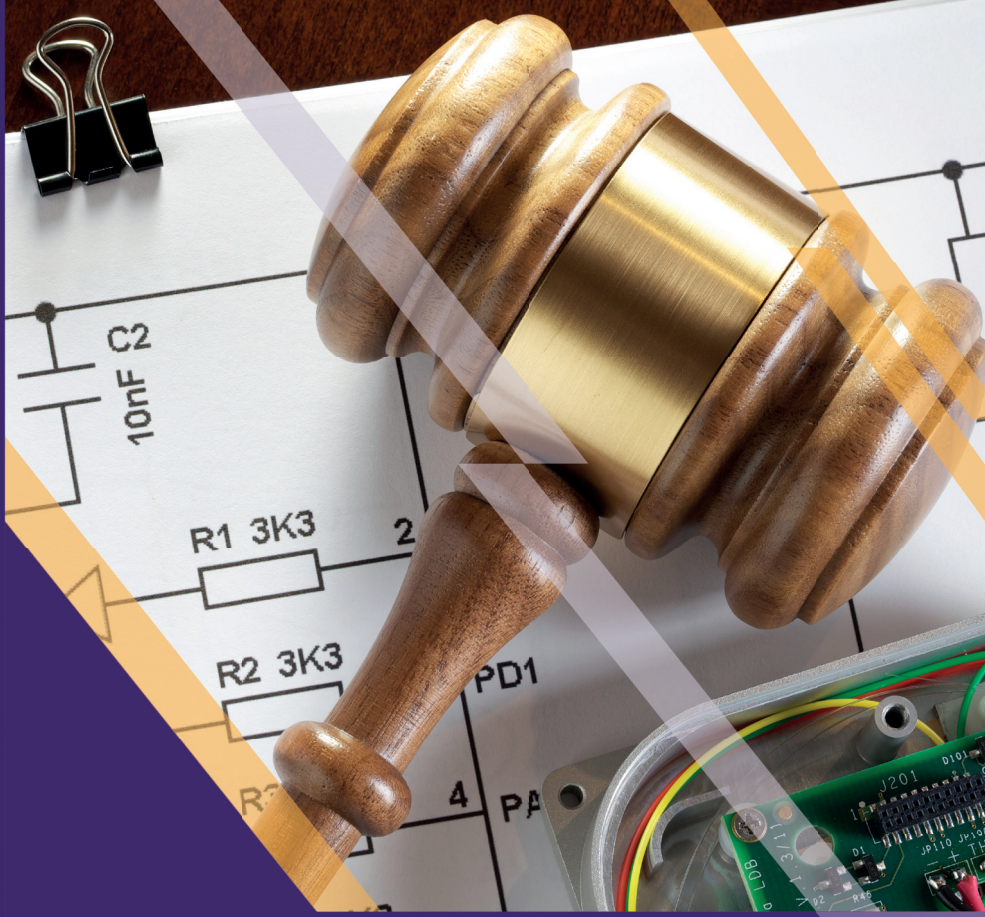

Direito Eletrônico

Direito eletrônico

Frederico Félix Gomes

Dados Internacionais de Catalogação na Publicação (CIP)

Gomes, Frederico Félix
G633d Direito eletrônico / Frederico Félix Gomes. – Londrina : Editora e Distribuidora Educacional S.A., 2017.
184 p.

ISBN 978-85-522-0213-4

1. Internet – Legislação - Brasil. I. Título.

CDD 343.8109944

2017
Editora e Distribuidora Educacional S.A.
Avenida Paris, 675 – Parque Residencial João Piza
CEP: 86041-100 — Londrina — PR
e-mail: editora.educacional@kroton.com.br
Homepage: http://www.kroton.com.br/

Sumário

Palavras do autor

Você sabia que, há pouco mais de quarenta anos, a internet como entendemos hoje era um projeto universitário? Que o termo "globalização" era impensável? Ou ainda que a transmissão de dados por fibra óptica ou satélites não passava de uma simples e longínqua ideia?

Ao longo desse período, nossa sociedade passou por transformações drásticas. A informação, que era antes um bem caro, pouco acessível e centralizado, passou a ser barata, extremamente acessível e compartilhada. Essa mudança de paradigma revolucionou diferentes segmentos da sociedade, inclusive o cotidiano forense. Precisamos, assim, refletir quanto à forma como o Direito é pensado, interpretado e exercido, dentro de um novo contexto de "Sociedade da Informação".

Nossos estudos em Direito Eletrônico objetivam desenvolver os conhecimentos relacionados a esse novo ramo jurídico, suas particularidades, principais características, interação com outros ramos jurídicos, além das implicações das novas tecnologias em conceitos do Direito há muito tempo consolidados.

Para tanto, na Unidade 1, iremos estudar a evolução da sociedade rumo a uma "Sociedade da Informação", o surgimento da internet e, consequentemente, do Direito Eletrônico, além de seus fundamentos e principais características, sua relação com outros ramos jurídicos e a problemática relacionada à regulação do espaço virtual no Brasil e no mundo. Traçaremos um espectro da Lei nº 12.965 de 2014, conhecida como "Marco Civil da Internet", analisando sua construção histórica, seus alicerces principiológicos, seus objetivos e os direitos e garantias consolidados por esse importante marco regulatório, com especial foco à neutralidade da rede.

Na Unidade 2, analisaremos o confronto entre direitos da personalidade na internet, em especial a privacidade e a liberdade de expressão, de modo a entender como resolver eventuais conflitos, analisando ainda a importância de cada uma; a formação de uma Sociedade Digital segura; e como o Marco Civil da Internet regula cada conflito. Estudaremos também a questão da responsabilidade civil dos provedores de internet, especialmente pelos atos praticados por terceiros.

Na Unidade 3, estudaremos questões ligadas à proteção da propriedade intelectual na internet, em face dos novos modelos de negócios. Especificamente, analisaremos a relação entre marcas e nomes de domínios e as controvérsias existentes no mercado de *streaming* de conteúdos protegidos por direitos autorais. Ademais, veremos questões relacionados ao e-commerce e à formação de contratos e títulos de créditos eletrônicos.

Por fim, na Unidade 4 analisaremos os problemas ligados aos delitos informáticos, inclusive envolvendo crianças e adolescentes, bem como a coleta de provas eletrônicas e breves noções de perícia forense computacional.

Se você ainda acha que a internet é uma "terra sem lei", nós o convidamos a embarcar nessa jornada de estudos que mostrará a interseção entre as inovações tecnológicas e mundo do Direito.

Introdução ao Direito Eletrônico e Marco Civil da Internet

Convite ao estudo

A troca facilitada de pacote de dados dentro de uma rede em escala mundial provocou mudanças drásticas em nossa sociedade. As informações passaram a circular de maneira irrestrita e em velocidade infinitamente superior. Podemos dizer que a internet foi um dos pilares do fenômeno da globalização e, por consequência, da própria evolução humana rumo à "Sociedade da Informação". A internet trouxe muitas facilidades que permitiram a interligação de empresas e pessoas estabelecidas em diferentes locais. Isso gerou transformações de cunho social, político e econômico.

A Ciência Jurídica, entendida como reflexo da sociedade em determinado tempo e local, também se transformou. Conceitos jurídicos rapidamente passaram a ser interpretados de uma nova maneira, consoante a nova realidade que vivemos, permeada pela tecnologia da informação.

Para entendermos como chegamos a esse estado atual, devemos compreender as raízes históricas da internet. A partir daí, iremos entender como o Direito Eletrônico se formou de maneira natural e como a rede mundial de computadores passou a ser regulada no Brasil, principalmente por meio do Marco Civil da Internet.

Para início dos nossos estudos, iremos considerar o seguinte contexto de aprendizagem: você foi contratado como consultor jurídico da Comissão de Ciência e Tecnologia do Senado. O senador "José da Telecom" apresentou um projeto de lei com objetivo de criar controles estritos sobre a internet brasileira. Umas das medidas propostas é a alteração do Marco Civil da Internet, com objetivo de criar exceções legais para a neutralidade da rede. Outra medida polêmica é a criação de

mecanismos legais para controle técnico da rede, tal como a criação de um modelo público de autenticação de acesso à rede através do número de CPF do usuário. Na condição de consultor jurídico, você deverá emitir um parecer contendo sua opinião legal acerca dos problemas advindos da regulação da internet, especificamente sobre os problemas trazidos pela criação de exceções legais ao princípio da neutralidade da rede e a adoção de tecnologias específicas na legislação.

Esse parecer será elaborado com a contribuição de cada situação-problema – (SP). Na SP 1, você deverá analisar os prós e os contras referentes à regulação da internet pelo Poder Público. Na SP 2, você deverá elaborar a segunda parte do parecer, analisando se a criação de um modelo público de autenticação de acesso à rede através do número de CPF do usuário é compatível com os princípios estabelecidos no Marco Civil da Internet. Na SP 3, você finalizará seu parecer, analisando a legalidade de um aplicativo *"zero rating"*.

Para dar uma ideia geral do que será tratado especificamente em cada seção desta Unidade 1, verifique que na Seção 1.1, iremos estudar a evolução da sociedade rumo a uma Sociedade da Informação, o surgimento da internet e, consequentemente, do Direito Eletrônico, além de seus fundamentos e principais características, sua relação com outros ramos jurídicos e a problemática relacionada à regulação do espaço virtual no Brasil e no mundo.

Na Seção 1.2, traçaremos um espectro da Lei nº 12.965 de 2014, conhecida como "Marco Civil da Internet", analisando sua construção histórica, alicerces principiológicos, seus objetivos e os direitos e garantias consolidados por esse importante marco regulatório, com especial foco à neutralidade da rede, que será aprofundada na Seção 1.3. Vamos, então, iniciar nossa jornada?

Seção 1.1

Posicionamento teórico do Direito Eletrônico

Diálogo aberto

Retomando nosso contexto de aprendizagem, o senador "José da Telecom" iniciou os trabalhos junto à comissão, convocando uma reunião entre todos os envolvidos. Tal reunião tem como principal objetivo ouvir a opinião dos especialistas no assunto sobre a pertinência desse projeto de lei (PL) e/ou para que eventuais mudanças neste sejam feitas.

Você foi selecionado para participar dessa reunião. Como sabemos, uma das medidas propostas é a alteração do Marco Civil da Internet, com objetivo de criar exceções legais para a neutralidade da rede. Outra medida polêmica é a criação de mecanismos legais para controle técnico da rede, como a criação de um modelo público de autenticação de acesso à rede através do número de CPF do usuário. Entretanto, antes mesmo de serem discutidos pontos específicos do projeto de lei, a Comissão de Avaliação do PL, da qual você faz parte, resolveu reunir-se para discutir os benefícios e malefícios advindos da regulação do espaço virtual. Além disso, se tais regulações teriam possível impacto (direto ou indireto) sobre outras leis. Assim, *você deverá emitir sua opinião apontando quais os prós e os contras referentes à regulação da internet pelo Poder Público.* Essa será a primeira parte de seu parecer jurídico, o seu produto. Para resolver essa situação-problema, você deverá observar as proposições teóricas de cada uma das Escolas do Direito Eletrônico estudadas nesta seção. Igualmente, para avaliar os possíveis impactos em outras leis, você deverá analisar a relação do Direito Eletrônico com outros ramos do Direito.

Não pode faltar

Antes de adentrarmos no estudo do Direito Eletrônico, precisamos traçar a linha evolutiva da própria internet, pois somente após a popularização da rede mundial de computadores é que o Direito Eletrônico, como ramo autônomo do Direito, começou a ganhar força. Isso porque as principais questões debatidas pelos especialistas no assunto originam-se a partir das próprias características da internet. Por isso, é fundamental entendermos o funcionamento da internet e como ela se tornou aquilo que é hoje.

> No que tange à história da internet propriamente dita, temos a primeira fase na década de 1960. Nela, começaram as pesquisas para a troca de mensagens em redes do tipo packet switched, ou seja, comunicações que se valiam de interligações lógicas, e não físicas, entre os usuários. Por sua vez, no ano de 1969, a Arpanet, uma rede de computadores de origem militar, criada pelo Departamento de Defesa dos Estados Unidos, já fazia o uso da tecnologia packet switched. Os computadores passaram a ser interligados à Arpanet ao longo dos anos seguintes a uma taxa acelerada (ROHRMANN, 2005, p. 5).

Entretanto, a internet como conhecemos hoje não teve sua origem exclusivamente na rede militar citada, uma vez que já se faziam pesquisas avançadas com redes de computadores *packet switched* na Universidade de Los Angeles e no Massachussets Institute of Technology (MIT). Até o início da década de 1970, a rede Arpanet ainda utilizava como protocolo para comutação de dados o chamado *Network Control Protocol* (NCP).

> Ocorre que o crescimento do número de computadores ligados à rede, ao longo da década de 1970, fez surgir um problema de natureza técnica: o protocolo NCP não protegia a rede contra a perda de pacotes de dados. Ou seja, se uma mensagem fosse dividida em diferentes pacotes e um deles se perdesse durante a transmissão, a mensagem apresentaria uma perda no recebimento. Havia, assim, a necessidade de um protocolo mais eficiente, capaz de detectar e corrigir erros referentes às perdas de dados ao longo da rede (ROHRMANN, 2005, p. 5).

Dessa necessidade surgiu o novo protocolo, TCP/IP, que é até hoje utilizado, encontrando-se atualmente em sua sexta versão (IPv6).

A década de 1980 foi marcada pela padronização do TCP/IP como protocolo da internet. Paralelamente, houve uma difusão elevada do uso da rede, principalmente pela comunidade científica, com o envolvimento das atividades acadêmicas e de pesquisa. Os usuários de então, ainda que provenientes de sistemas de computadores diferentes, já faziam uso maciço do e-mail.

Por sua vez, a década de 1990 começa com o fechamento da Arpanet, sendo que a gerência da rede passou a ser exercida pela

National Science Foundation (NSF). Foi também o marco do início da maior utilização da internet pelas pessoais naturais e jurídicas. O grande crescimento da internet entre os usuários não ligados às atividades de pesquisa deu-se em razão de dois fatores essenciais (ROHRMANN, 2005, p. 6).

O primeiro foi a popularização da *World Wide Web* (WWW), graças ao surgimento de programas capazes de manipular interfaces gráficas. Tornou-se mais fácil (e agradável) a comunicação de dados pela internet. O segundo fator foi o surgimento dos provedores de acesso, isto é, empresas que possibilitam o acesso do público em geral à internet – assunto da Unidade 2 deste curso.

A década de 1990 coincide, ainda, com a publicação dos primeiros artigos e textos jurídicos sobre a aplicação do Direito à rede mundial de computadores. As primeiras discussões tratavam sobre o conflito de jurisdição no espaço virtual. Uma vez que as pessoas acessam *websites* localizados em outros países e praticam atos jurídicos nesses locais (ex.: sites de apostas), o problema da jurisdição ganhou particular destaque.

O Direito "comum" (entendido como aquele praticado desde tempos medievos) não conseguia resolver alguns problemas antes considerados básicos (ex.: jurisdição), surgindo daí a necessidade de um ramo jurídico diferenciado, marcado notadamente pela necessidade de conhecimentos técnicos acerca de conceitos computacionais, bem como sobre a própria estrutura da rede mundial de computadores. Nasceu a partir daí o "Direito Eletrônico", conhecido também como "Direito Digital" ou "Direito Virtual".

Nesse diapasão, "o principal objetivo desse novel ramo jurídico é justamente apresentar soluções para as novas situações de conflitos trazidas pela virtualização de grande número de atos jurídicos". (ROHRMANN, 2005, p. 9).

De acordo com Pinheiro, assimile o conceito de Direito Eletrônico:

> **O Direito Eletrônico ou Direito Digital consiste na evolução da própria ciência jurídica, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas. (PINHEIRO, 2016, p. 77)**

Percebe-se que a rede mundial de computadores surgiu em território estadunidense. Da mesma forma, o número de sites em inglês preponderava em relação às demais línguas, além do fluxo de dados na América do Norte ser preponderante em relação às outras regiões. Surgiu, assim, uma preocupação acadêmica de o Direito norte-americano ser utilizado como principal fonte de Direito aplicável às relações que fizessem uso da rede.

Ao mesmo tempo, houve uma reação contrária ao uso do "direito do mundo físico" como o Direito da Internet. Essa primeira reação surgiu da teoria segundo a qual a internet criaria "comunidades" próprias, alheias ao mundo físico. A ideia de "comunidade da internet" ganhou, pois, respaldo em um setor da academia jurídica, especialmente nos Estados Unidos. Tal fato coincide com a criação da primeira corrente ou escola do Direto Eletrônico, que propunha um Direito próprio para a rede, chamada de "corrente libertária".

A "corrente libertária" encontra como principais expoentes autores como Barlow, Post e Johnson, que ganharam projeção com artigos que questionavam justamente a eficácia do "direito tradicional" para regulamentar os ambientes digitais. Certamente, o documento que melhor simboliza e resume os pensamentos dessa corrente é a consagrada *Declaração de Independência do Ciberespaço*, publicada em 8 de fevereiro de 1996, cuja autoria pertence a John Perry Barlow.

Pesquise mais

Indicamos a leitura do inteiro teor da *Declaração de Independência do Ciberespaço*, disponível em: <http://www.dhnet.org.br/ciber/textos/barlow.htm> (acesso em: 17 abr. 2017). Nesse documento, Barlow afirma que "o espaço cibernético consiste em ideias, transações e relacionamentos próprios, tabelados como uma onda parada na rede das nossas comunicações" e que "nosso é um mundo que está ao mesmo tempo em todos os lugares e em nenhum lugar, mas não é onde pessoas vivem". Percebe-se que a questão da territorialidade, antes tão bem compreendida pela ciência jurídica, é questionada, impondo novos desafios aos operadores do Direito desde aquela época.

A teoria libertária pode ser resumida em sua própria essência: a negação da autoridade do Estado em ambiente eletrônico "desprovido de territorialidade" e dotado de uma "soberania própria" (WU, 1997, p. 647).

Muitas críticas foram feitas a essa corrente. A principal reside no fato de ela definir o espaço virtual como um local separado do "mundo real", ou seja, como um local próprio, fora do controle dos Estados. Nesse sentido, não se poderia crer no surgimento de um Estado "separado do mundo físico" apenas porque se criou uma rede de comunicação, tal qual a internet, que interliga vários usuários e Estados diferentes.

Após duras críticas da comunidade jurídica à Escola Libertária, surgiu a segunda corrente, chamada de "Escola da Arquitetura da Rede". Tal corrente tem por principal autor o professor Lawrence Lessig. A ideia básica que circunda esse pensamento se apoia na necessidade do próprio Estado de determinar a natureza tecnológica do espaço virtual, para que, assim, se possa regulamentar a internet, essencialmente por meio do Direito e, dessa forma, evitar que uma empresa provedora de serviços exerça um controle maior sobre a rede, através da arquitetura da programação, e de forma alheia à vontade do Estado. Todavia, a própria corrente reconhece algumas dificuldades para regulamentação jurídica do espaço virtual, principalmente em face de algumas características técnicas do ambiente eletrônico, como a ausência de limites territoriais e o dinamismo da rede.

Nesse diapasão, Lessig defende a tese de que o espaço virtual não teria "natureza predefinida". Pelo contrário, aquilo que irá determinar essa "natureza" é o "código" (*code*). Mas não os códigos legais, como o Código Civil ou o Código Penal, e sim o código de programação de computador, que cria e molda a forma como usuários interagem na rede. Ademais, a determinação da arquitetura da rede, ou seja, a condução da programação da internet, não poderia ser deixada a cargo exclusivo dos entes privados, pois a ausência de intervenção do Poder Público acabaria por acarretar o controle maior da internet por esses provedores, sendo tal fato nocivo aos demais usuários, uma vez que a tendência é que os provedores busquem atender aos próprios interesses econômicos (LESSIG, 1999).

Apesar de essa corrente encontrar apoiadores até os dias atuais, algumas críticas foram feitas às suas ideias. A principal diz que ela não considera o Direito como a melhor forma de solução de conflitos sociais, a qual é elaborada para o bem comum e oriunda de um poder estatal, detentor do monopólio da força ou coerção. Assim, pode-se dizer que, embora não admitido pelos seus doutrinadores, essa corrente traz em seu âmago a utopia de um espaço virtual onde as pessoas vivem em relativa harmonia e que os conflitos sociais

poderiam ser mitigados através do próprio código de programação. Entendemos tal ideal como utópico, uma vez que a proximidade entre os usuários, possibilitada pela própria arquitetura da rede, potencializa os conflitos já existentes na sociedade, sendo que os provedores de serviços, donos dessa arquitetura, não têm interesse em resolvê-los de forma imparcial, tal qual o Poder Judiciário.

Por sua vez, temos uma terceira corrente, intitulada de corrente do "Direito Internacional", que idealiza o espaço virtual como um verdadeiro "território internacional", tendo em vista a facilidade de uma pessoa ter acesso a recursos dispostos em *websites* estrangeiros sem ter que deixar, fisicamente, o seu próprio país. Para essa corrente, o espaço virtual deveria ser objeto de regulamentações internacionais, seja por usos e costumes internacionais, seja por tratados do tipo dos que são usados no Direito Marítimo, por exemplo. Suas críticas referem-se a sua difícil aplicabilidade prática, já que certos atos são mais bem regulados por normas de direito interno, sobretudo aqueles referentes a atos privados, como contratos, além de mecanismos falhos de *enforcement*, ou seja, mecanismos que tornam executável determinada decisão ou norma.

Finalmente, chegamos à corrente "Tradicionalista". Lembre-se de que as duas correntes anteriores surgiram justamente em razão das dificuldades de aplicação do Direito tradicional ao ambiente eletrônico. A corrente tradicionalista não nega necessariamente tais dificuldades, mas entende que o Direito é muito mais amplo do que a simples possibilidade de aplicação da norma em uma situação concreta e específica. Nesse sentido, o Direito possui características próprias, que o distingue de outros sistemas de regras, tais como a busca da justiça e do bem comum; sua autoridade universal; e sua aplicação por um ente detentor de força coercitiva, qual seja, o Estado. Por isso, essa corrente defende que o espaço virtual não é um local separado do mundo físico, como pensam os libertários, e também que as regras baseadas no código de programação não são suficientes para coibir determinadas condutas, como pensam os autores ligados à escola da arquitetura da rede. Ora, os mesmos criadores dos códigos detêm a habilidade para contorná-los. Igualmente, a aplicação do Direito pelo Estado supriria a questão da aplicabilidade prática, ponto fraco da corrente do Direito Internacional.

A corrente Tradicionalista propõe a aplicação do Direito aos fatos jurídicos que ocorrem no espaço virtual. A maior crítica que se faz a essa corrente reside no fato de que os operadores do Direito, inclusive

seus criadores, em sua ampla maioria, não possuem conhecimentos técnicos suficientes para criar e aplicar normas jurídicas, de maneira correta, às diferentes situações ocorridas no espaço eletrônico e, ainda, que os legisladores, muitas vezes, atuam em prol de interesses privados, nem sempre visando ao bem comum.

Assim, com exceção da escola Libertária, todas as outras defendem a possibilidade de regulação do espaço virtual. Dessa forma, podemos estudar melhor o Direito Eletrônico sem preocupação com a chamada "impossibilidade" de regulamentação do meio eletrônico.

Ato contínuo, sempre que determinada área jurídica começa a ser estudada com mais especificidade, surge a dúvida se ela se trataria, ou não, de um ramo autônomo do Direito. A questão da análise da autonomia de determinado ramo do Direito passa essencialmente pela busca de princípios próprios, que informem o pretenso ramo autônomo. Outros parâmetros que são utilizados para justificar essa autonomia são: um corpo legislativo próprio e destacado; os casos que são decididos acerca da matéria; e até mesmo o estudo da disciplina em cursos de graduação ou pós-graduação (ROHRMANN, 2005).

Ao nosso ver, existem fatores que levam a classificar o Direito Eletrônico como um ramo autônomo do Direito. Entre tais fatores, destacamos: a maciça produção acadêmica nacional sobre o tema; a erupção de vários diplomas legais no Brasil e no mundo, tanto na esfera legislativa, quanto executiva; além de casos julgados pelo Poder Judiciário, com cada vez mais especialidade sobre o assunto.

Nesse sentido, a autonomia do Direto Eletrônico poderia decorrer também da chamada "excepcionalidade da internet". Esse conceito nos leva à seguinte reflexão: O que faz a internet tão "especial" a ponto de ser tratada de maneira diferente de outras mídias, como rádio ou TV, que possuem inúmeras regulações? A internet é realmente uma exceção? Quais os perigos de regulá-la da mesma maneira que regulamos outros setores, como a telefonia? (GOLDMAN, 2008).

Todavia, apesar de autônomo, o Direito Eletrônico relaciona-se intimamente com outros ramos do Direito. A onipresença da tecnologia da informação nas várias relações e situações do cotidiano demarcam essa característica própria do Direito Eletrônico, qual seja, sua "multidisciplinaridade", consubstanciada na influência dos diversos outros ramos jurídicos na formação deste ramo "especial".

Exemplificando

A título de exemplo, citamos a seguir alguns ramos do Direito e sua relação com o Direito Eletrônico:

a) Direito Civil: O estudo da responsabilidade civil por atos ilícitos praticados por meio eletrônico é um exemplo da relação entre os dois ramos;

b) Direito Penal: A criminalização de algumas condutas praticadas por meio eletrônico, como o acesso não autorizado ao dispositivo informático (Art. 124-A do Código Penal) tem relação direta com o Direito Eletrônico;

c) Direito Processual: A questão da produção de prova a partir do meio eletrônico e sua validade jurídica é um tema que desperta muito interesse entre estudiosos de ambas as áreas;

d) Direito Constitucional: O eterno embate entre o direito à privacidade e o direito à liberdade de expressão.

Portanto, conclui-se que o surgimento e a consolidação do Direito Eletrônico como ramo autônomo do Direito coincidem com a própria consolidação e popularização da internet, que trouxe diversas novas situações, as quais os operadores do Direito não estavam acostumados, e cuja resolução demanda conhecimentos técnicos específicos acerca do próprio funcionamento da rede.

Reflita

Considerando a revolução digital ocorrida nas últimas décadas, aliada à difusão do uso da rede mundial de computadores, você considera ser o Direito Eletrônico ramo específico do Direito? Ou seria simplesmente mero "reflexo" da tecnologia da informação nos ramos mais tradicionais, como Civil, Tributário, Trabalhista, etc.? Quais outros fatores você consegue pensar que justificariam tal enquadramento autônomo?

Sem medo de errar

Pois bem, caro aluno, lembro que *você* deverá emitir sua opinião apontando os prós e os contras referentes à regulação da internet pelo Poder Público. Vamos, então, agora à resolução da nossa situação-problema (SP)?

Primeiramente, devemos relembrar a estrutura de um parecer jurídico. Trata-se de documento com estrutura livre e segmentada

por temas, ou questionamentos, os quais devem ser respondidos conforme sua opinião legal, acerca de determinados temas. O primeiro tema a ser tratado tanto no parecer quanto na Reunião citada na situação-problema refere-se à regulação do espaço virtual pelo Poder Público, especificamente as vantagens e desvantagens advindas dessa regulação.

Pois bem. Após estudarmos as Escolas do Direito Eletrônico, temos capacidade para realizar tais apontamentos. Para termos uma melhor visualização da resposta, iremos utilizar o formato de tópicos. Então, a primeira parte de seu parecer deverá seguir o seguinte modelo:

QUESTÕES A SEREM RESPONDIDAS NO PARECER:

- QUAIS OS PRÓS E CONTRAS DA REGULAÇÃO DA INTERNET PELO PODER PÚBLICO, CONFORME PROPOSTO NO PROJETO DE LEI?

Resposta: A regulação do espaço eletrônico e, consequentemente, da internet é assunto que gera debates desde a própria origem do Direito Eletrônico, que remonta à década de 1990. Para respondermos essa questão, é necessário analisar os argumentos utilizados por cada uma das correntes (ou Escolas) do Direito Eletrônico:

a) Para a corrente libertária, que defende a criação de um direito próprio para a internet, **não teríamos vantagens** na regulação do espaço virtual pelo Poder Público, tendo em vista a ausência de autoridade do Estado em ambiente eletrônico, o qual é "desprovido de territorialidade" e dotado de uma "soberania própria", sendo impossível a aplicação do Direito tradicional. Elas podem ser também entendidas como as desvantagens da regulação da internet.

b) Para a escola da arquitetura da rede, que se apoia na ideia da necessidade de o Estado determinar a natureza tecnológica do espaço virtual para que se possa regulamentar, por meio do Direito, o mundo on-line e, desta forma, evitar que alguém do mercado determine um controle maior sobre a rede, pelo tipo de programação, de forma alheia à vontade do Estado, **a vantagem** da regulação do espaço virtual reside no fato de que a ausência de intervenção do Estado acabaria por acarretar controle maior desses entes, o que seria nocivo para os demais usuários, tendo em vista que os provedores buscariam sempre atender aos próprios interesses econômicos.

c) Para a corrente do Direito Internacional, o espaço virtual deveria ser regulado por meio de regulamentações internacionais, usos e costumes internacionais, além de tratados do tipo dos que são usados, por exemplo, no Direito Marítimo, pois tais fontes do Direito são conhecidas por todos os Estados e consequentemente os usuários.

d) Para a escola Tradicionalista, como o espaço virtual é uma "extensão" do mundo físico, as mesmas normas se aplicariam, trazendo **vantagens** como a uniformidade das relações entre usuários e, consequentemente, maior segurança jurídica. A **desvantagem** reside no fato de que os operadores do Direito muitas vezes não detêm conhecimentos técnicos suficientes para resolver determinadas questões relacionadas a esse ambiente.

De maneira sintética, as **vantagens** da regulação seriam:

• Maior segurança jurídica, por meio do uso de normas do mundo físico, advindas tanto de normas de Direito Internacional, como de Direito Interno.

• Existência de uma "força coatora", eis que a ausência de intervenção do Estado acabaria por acarretar controle maior pelos provedores de internet, o que seria nocivo para os demais usuários, tendo em vista que os provedores buscariam sempre atender aos próprios interesses econômicos.

Já as **desvantagens** seriam:

• Operadores de Direito, inclusive os legisladores, muitas vezes não detêm conhecimentos técnicos suficientes para resolver determinadas questões relacionadas ao ambiente eletrônico.

• Uma vez que o ambiente eletrônico é "desprovido de territorialidade" e dotado de uma certa "soberania própria", seria impossível a aplicação do Direito Tradicional, não sendo recomendável sua regulação.

Avançando na prática

Criação de Vara Especializada em Direito Eletrônico

Descrição da situação-problema

Ainda na condição de consultor jurídico especializado, você foi procurado pelo presidente do Tribunal de Justiça de São Paulo para emitir sua opinião sobre a necessidade (ou não) de criação de Varas Especializadas em Direito Eletrônico, para atender demandas específicas sobre o tema. As principais dúvidas do presidente referem-

se justamente à concepção do Direito Eletrônico como um ramo autônomo do Direito, bem como se as Varas Cíveis e/ou Penais não são suficientes para a resolução de questões relacionadas ao tema.

Resolução da situação-problema

As dúvidas referentes à criação de Varas especializadas em Direito Eletrônico passam justamente pela própria classificação desse ramo como um ramo autônomo do Direito. Lembre-se de que quando determinada área começa a ser estudada com mais especificidade, surge a dúvida se se trataria, ou não, de um ramo autônomo do Direito. Nesse sentido, a questão da análise da autonomia de determinado ramo do Direito passa essencialmente pela busca de princípios próprios, que embasem o pretenso ramo autônomo.

Outros parâmetros que podem ser utilizados na busca da demonstração da autonomia referem-se a um corpo legislativo próprio, destacado, aos casos que são decididos acerca da matéria e até mesmo ao estudo da disciplina em cursos de graduação ou pós-graduação.

Se não bastasse, existem fatores que nos levam a entender o Direito Eletrônico como um ramo autônomo do Direito, dos quais destacamos: a grande produção acadêmica nacional sobre o tema; o surgimento de vários diplomas legais no Brasil e no mundo, tanto na esfera legislativa, quanto executiva; além de casos julgados pelo Poder Judiciário, com cada vez mais especialidade sobre o assunto.

Podemos ainda considerar que, embora o Poder Judiciário esteja cada vez mais inteirado sobre tais assuntos, diversos operadores do Direito não detêm conhecimentos técnicos suficientes para resolver determinadas questões relacionadas ao ambiente eletrônico. A população em geral se beneficiaria da criação dessas Varas Especializadas.

Faça valer a pena

1. Até o início da década de 1970, a rede Arpanet ainda utilizava como protocolo para comutação de dados o chamado *Network Control Protocol* (NCP). Ocorre que o crescimento do número de computadores ligados à rede, ao longo da década de 1970, fez surgir um problema de natureza técnica: o protocolo NCP não protegia a rede contra a perda de pacotes de dados. Havia, assim, a necessidade de um protocolo mais eficiente, capaz de detectar e corrigir erros referentes às perdas de dados ao longo da rede.

Assinale a alternativa que apresenta o protocolo que veio a substituir o NCP e que é utilizado até os dias de hoje:
a) FTP.
b) SSH.
c) SMTP.
d) TCP/IP.
e) IMAP.

2. A internet surgiu como uma rede eminentemente norte-americana. Se não bastasse, o número de sites em inglês preponderava em relação à demais línguas e o fluxo de dados na América do Norte era significativo. Surgiu, pois, uma preocupação acadêmica de o Direito norte-americano ser utilizado como principal fonte de Direito aplicável às relações que fizessem uso da rede. Concomitantemente, houve uma reação contrária ao uso do "direito do mundo físico" como o Direito da internet. Essa primeira reação surgiu da teoria segundo a qual a internet criaria "comunidades" próprias, alheias ao mundo físico. A ideia de "comunidade da internet" ganhou, pois, respaldo em um setor da academia jurídica, especialmente nos Estados Unidos. Surgiu, assim, a primeira corrente teórica (ou Escola) do Direito Eletrônico.
Sobre as correntes do Direito Eletrônico, assinale aquela que preconiza que as normas de Direito Interno devem ser utilizadas para regulação do espaço virtual, tendo em vista este tratar-se de mera extensão do mundo físico:
a) Corrente do "Direito Internacional".
b) Corrente "Libertária".
c) Escola da "Arquitetura da Rede".
d) Corrente "Tradicionalista".
e) Escola da "Programação Controlada".

3. A presença da tecnologia da informação nas várias situações do cotidiano demarcam uma característica muito interessante do Direito Eletrônico, qual seja, sua multidisciplinaridade, consubstanciada na influência dos diversos outros ramos jurídicos na formação desse ramo "especial".
O estudo da responsabilidade dos provedores por atos ilícitos praticados por meio eletrônico é um exemplo da relação entre o Direito Eletrônico e qual dos ramos do Direito a seguir elencados?
a) Direito Penal.
b) Direito Empresarial.
c) Direito Civil.
d) Direito Trabalhista.
e) Direito Previdenciário.

Seção 1.2

Regulação do espaço virtual

Diálogo aberto

Você sabia que, até os dias de hoje, temos relato de pessoas que acreditam que a internet é um verdadeiro "velho oeste", uma "terra sem lei", onde todos podem fazer aquilo que bem entendem sem nenhum tipo de punição? Apesar de ser um pensamento antigo, ele ainda está presente. Tal fato se dá essencialmente pela novidade das leis que visam regular o espaço virtual, aliada às dificuldades inerentes à interpretação e aplicação de normas já existentes às situações concretas ocorridas no ambiente digital. Mas será que toda regulação é bem-vinda?

Como sabemos, um dos propósitos do projeto de lei descrito em nosso contexto de aprendizagem é a criação de mecanismos legais para controle técnico da rede, especificamente a criação de um modelo público de autenticação de acesso à rede por meio do número de CPF do usuário. Tal medida criou uma polêmica muito grande com a ONG Defensores da Privacidade Online. Eles argumentam que tal medida violaria o direito constitucional à privacidade dos cidadãos e usuários da internet. Automaticamente, você foi consultado para dar sua opinião legal, na forma de parecer, analisando se a criação de um modelo público de autenticação de acesso à rede por meio do número de CPF do usuário é compatível princípios estabelecidos no Marco Civil da Internet ou se haveria alguma solução alternativa visando mitigar a impunidade no espaço digital.

Para resolver essa situação-problema, iremos estudar como se deu o processo de regulação da rede no Brasil, comparando-o brevemente com outras iniciativas ao redor do mundo, bem como iremos analisar os fundamentos, princípios e objetivos estabelecidos no Marco Civil da Internet, além dos direitos e garantias dos usuários no uso da internet, para assim formarmos nossa opinião legal acerca da legalidade de iniciativas como aquela descrita no contexto de aprendizagem, qual seja, criação de um modelo público de autenticação de acesso à rede por meio do número de CPF do usuário.

Esta será a segunda parte de seu parecer jurídico, o seu produto, lembrando que, conforme explicado na Seção 1.1, o parecer consiste na resposta de perguntas feitas pelo consulente ao especialista.

Não pode faltar

Como vimos na Seção 1.1, a tecnologia da informação evoluiu num ritmo frenético, principalmente na última metade do século XX, tornando-se cada vez mais complexa e acessível à população mundial, embora muito ainda tenha a evoluir. Nas décadas de 1960 e 1970, houve a idealização da internet e suas peculiaridades comunicativas céleres e constantes inovações, e, a partir década de 1990, mais especificamente após a criação da World Wide Web, a internet se tornou usual em todo o planeta. No Brasil, passou a ser mais usual a partir de 1995, quando deixou de ser de uso exclusivo das universidades e passou a ter acesso público e também quando foi criado o Comitê Gestor da Internet no Brasil (CGI.br), pela Portaria Interministerial nº 147, de 31 de maio de 1995, alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003.

Tendo em vista que o uso da internet pela sociedade civil ocorre desde meados da década de 1990, pode-se dizer que o país tardou em elaborar uma legislação específica para regular minimamente as interações no ambiente virtual.

A normatização da internet demorou a ser concluída não só pela natural morosidade do processo legislativo brasileiro, mas também porque a matéria envolve uma clara disputa de interesses entre o mercado, que deseja liberdade para operar nesse segmento; a sociedade civil, que teme e repudia qualquer restrição à liberdade de expressão; e o Estado, cujo Poder Legislativo parecia não dispor de conhecimento suficiente para propor uma legislação sobre o tema.

Perceba que as dificuldades para a regulação da internet no Brasil citadas remontam às próprias críticas às correntes do Direito Eletrônico. O interesse do mercado representa um pivô na questão da regulação da rede pelo código de programação, conforme proposto pela escola da Arquitetura da Rede. Já a dificuldade natural do Poder Legislativo remonta às críticas feitas à escola Tradicionalista.

Não obstante tais dificuldades, em 2009 foi feita uma parceria entre a Secretaria de Assuntos Legislativos do Ministério da Justiça e a Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, com objetivo de dar início a um processo colaborativo de construção de uma proposta ou minuta de lei. Para tanto, foi desenvolvida uma plataforma na internet, hospedada no site "culturadigital.br", onde

inicialmente foi divulgado um texto-base produzido pelo Ministério da Justiça, no qual identificava e propunha a sistematização dos principais temas referentes à internet que se encontravam pendentes de regulação no país.

Partindo dessa publicação, membros do governo, sociedade civil, representantes dos provedores de serviços na internet, membros da academia e demais interessados no tema foram incentivados a debater e publicar suas contribuições, num processo inédito de construção coletiva que resultou na proposta inicial e embrionária de uma legislação para a internet brasileira, que posteriormente consolidou-se na minuta atual da Lei nº 12.965 de 2014, conhecida como Marco Civil da Internet (MCI).

Assimile

O Marco Civil foi idealizado como um projeto de lei singular. Não apenas por conta de seu conteúdo, mas também pelo seu processo de criação, debate e aprovação. O Marco Civil estabeleceu princípios, direitos e deveres para a rede no Brasil de forma articulada com os princípios da democracia (LEMOS, 2015). O inteiro teor do texto aprovado do MCI está disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> (acesso em: 28 abr. 2017).

A forma como a internet é regulada juridicamente em diferentes países possui orientações muito distintas. Ao mesmo tempo em que o Marco Civil era aprovado no Brasil, democracias como a Turquia e a Rússia adotaram leis que despontam em sentido completamente oposto. São textos legais que aumentam o controle sobre a internet por parte do Poder Executivo; que estabelecem mecanismos de controle das informações publicadas na rede sem o escrutínio do Poder Judiciário; ou ainda, que criam regimes semelhantes à censura, punindo usuários que divergem politicamente do poder em exercício.

Não é mera coincidência que essas leis – adotadas por outras duas relevantes nações globais – tenham sido aprovadas com poucos dias de diferença do Marco Civil da Internet. Presenciamos um momento em que diversos países estão revisando seus marcos regulatórios para a rede, com efeitos e objetivos diferentes. Em face desse contexto, a importância da lei brasileira revela-se ainda maior quando comparada com esse cenário internacional de depreciação de direitos na rede. Ao contrário de Turquia e Rússia (além de outros países como China,

Irã, Arábia Saudita e Tailândia), nosso país aprovou uma arquitetura legislativa fundada na adoção de freios e contrapesos (LEMOS, 2015).

O escopo foi justamente assegurar liberdades públicas, limitando o poder do Executivo de interferir na rede brasileira, concretizando assim os preceitos da Constituição Federal de 1988.

Adentrando um pouco mais no conteúdo normativo do Marco Civil da internet, verificamos que seu artigo 1º define o objetivo principal desse novel diploma legal, qual seja, estabelecer "princípios, garantias, direitos e deveres para o uso da internet no Brasil" e determinar "as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria" (BRASIL, 2014, art. 1º).

Perceba que a lei estabelece primeiramente "princípios", para somente depois mencionar "garantias, direitos e deveres". Coerentemente, o Capítulo I da lei cuida dos fundamentos, dos princípios, dos objetivos, dos conceitos aplicáveis a esta. A simples leitura do Capítulo I leva à conclusão de que ele, por possuir caráter principiológico, enforma todos os demais capítulos, que possuem outras regras importantes, como responsabilidade de provedores, guarda de registros de conexão e aplicação, etc. Daí a importância do estudo das disposições preliminares contidas na Lei, para que possamos interpretar, de maneira coerente, o restante das normas contidas no diploma legal em análise, além de possibilitar nossa resposta à situação-problema proposta no início da seção, relembrando que iremos precisar analisar os próprios princípios do MCI em nossa resposta.

Apesar de haver diferenças jurídico-filosóficas entre os termos "princípios", "fundamentos" e "objetivos", os quais foram estudados no curso de Introdução ao Estudo do Direito, com relação ao Marco Civil da Internet, interpretam-se tais acepções de maneira harmônica, sendo que em determinados momentos um mesmo princípio pode assumir o manto de fundamento ou garantia.

Exemplificando

A liberdade de expressão aparece no texto do Marco Civil da Internet ora como fundamento, ora como princípio, nos artigos 2º e 3º respectivamente, bem como garantia do usuário, no artigo 8º. O legislador foi bem enfático ao reiterar a necessidade de proteção à

liberdade de expressão. Tal princípio vem sendo constantemente atacado por tentativas de aprovação de leis que vulneram a liberdade do cidadão. Apesar de raro, ainda vemos decisões judiciais que visam remover conteúdos de sites e blogs simplesmente por tornarem pública uma opinião política divergente.

O artigo 2º do Marco Civil da Internet traz como fundamento do uso da internet no Brasil o respeito à liberdade de expressão, bem como o reconhecimento da escala mundial da rede; os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; a pluralidade e a diversidade; a abertura e a colaboração; a livre iniciativa, a livre concorrência e a defesa do consumidor; e a finalidade social da rede.

Já em seu artigo 3º, a lei estabelece os seguintes princípios para o citado uso da rede: garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; proteção da privacidade; proteção dos dados pessoais; preservação e garantia da neutralidade de rede; preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; responsabilização dos agentes de acordo com suas atividades; preservação da natureza participativa da rede; liberdade dos modelos de negócios promovidos na internet.

Reflita

Você acha que algum desses princípios pode ser aplicado para colocar barreiras a iniciativas legislativas semelhantes àquela descrita na situação-problema?

Por sua vez, a disciplina do uso da internet no Brasil tem por objetivo, conforme o artigo 4º da lei, a promoção: do direito de acesso à internet a todos; do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos; da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

A leitura dos artigos citados nos leva a crer que o Marco Civil foi, de fato, pensado como um instrumento jurídico para promover uma internet livre e aberta, o que o torna um documento de vanguarda, inclusive em escala global.

Antes de analisarmos o Capítulo II do Marco Civil, que estabelece os direitos e garantias dos usuários, é importante destacarmos o artigo 6º, que traz uma norma interpretativa da lei, *in verbis*:

> **Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural. (BRASIL, 2014)**

Este artigo dá ao magistrado um comando muito claro: na tarefa de interpretação de um determinado dispositivo legal, ele deverá orientar-se com os fundamentos descritos no artigo 2º, com os princípios estampados no artigo 3º e de acordo com os objetivos previstos no artigo 4º. Entretanto, além disso, deverá levar em conta a "natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, cultural, social e econômico" (DE LUCCA, 2015, p. 75).

Reflita

Decisões envolvendo o bloqueio de aplicações como o WhatsApp tornaram-se comuns após o advento do Marco Civil da Internet, tendo como fundamento o artigo 12, inciso III, da citada lei. Na sua opinião, a interpretação dos magistrados sobre essa norma é razoável ou mesmo compatível com o disposto no artigo 6º da mesma lei? O bloqueio temporário de aplicações pelo Judiciário é válido a partir de uma interpretação dos princípios que formam o Marco Civil da Internet?

Ato contínuo, o Capítulo II da Lei nº 12.965 de 2014 traz em seus artigos 7º e 8º os direitos e garantias dos usuários. Interessante notar que o artigo 7º dispõe, logo no início, que o acesso à internet é "essencial ao exercício da cidadania". Tal passagem representou um avanço muito grande, pois colocou em destaque ferramentas que possibilitam o chamado *e-government*, que nada mais é do que a aproximação entre governantes e governados através de recursos

tecnológicos, sobretudo conectados via rede. Igualmente, o acesso à internet foi alçado ao patamar de direito fundamental, ao passo que se tornou essencial para a consecução da cidadania.

Ficaram assegurados os seguintes direitos aos usuários da internet:

a) inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

b) inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial;

c) inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

d) não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

e) manutenção da qualidade contratada da conexão à internet;

f) informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

g) não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

h) informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades específicas;

i) consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

j) exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

k) publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

l) acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, e;

m) aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Importante ressaltar que a Lei n.º 13.709, de 14 de agosto de 2018, a Lei de Proteção de dados, introduziu algumas alterações nos artigos 7º e 16º do Marco Civil da Internet . Essa lei tem como fundamento a proteção dos direitos fundamentais de liberdade, privacidade e do livre desenvolvimento da personalidade da pessoa natural. Assim, foca na transparência e a segurança no tratamento de dados pessoais, inclusive nos meios digitais, seja na coleta ou na utilização, de pessoas naturais ou jurídicas de direito público ou privado.

Já o artigo 8º estabelece que o exercício do direito de acesso à internet tem como condição a garantia do direito à privacidade e liberdade de expressão, sendo que eventuais cláusulas contratuais que violem tais direitos poderão ser consideradas nulas. O parágrafo único estabeleceu rol exemplificativo de cláusulas, tais como aquelas que "impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet" ou "em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil" (BRASIL, 2014, [s.p.]).

Esta última nos parece um exemplo, no mínimo, forçado, eis que o foro de solução de controvérsias desponta muito mais para o aspecto processual do direito. A tarefa de conceber uma cláusula de foro capaz de violar o direito de privacidade ou liberdade de expressão é tarefa complexa. Parece que o legislador teve por objetivo forçar a aplicação da legislação brasileira para provedores de aplicação localizados no exterior, de modo que estes busquem cumprir aquilo estabelecido em lei.

Em conclusão, vimos que o Marco Civil da Internet representou um grande avanço para a questão da regulação do espaço virtual, ocasionando maior segurança jurídica para usuários, empresas, governantes, magistrados e demais envolvidos na rede. Igualmente, a lei estabeleceu garantias de uma internet livre e aberta, representando importante alicerce no combate às iniciativas antidemocráticas, como aquelas adotados na Turquia e na Rússia.

Pesquise mais

Para saber mais sobre a Lei de Proteção de dados, acesse: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 4 nov. 2018.

Por fim, vimos alguns conceitos gerais que o Marco Civil da internet trouxe, consolidando ideais que vêm permeando as discussões globais quanto à regulação da rede. Reitere-se que o MCI foi definitivamente um marco em nossa história, bem como na história da internet mundial, tendo em vista que vem sendo utilizado como exemplo para outras legislações de diversos outros países. Ao que nos parece, o mesmo acontecerá com a Lei de Proteção de Dados, um novo paradigma para que ora os cidadãos possam saber como e quais dos seus dados são coletados; ora para as empresas em desenvolver canais para fornecer essas informações de forma clara, bem como capacitar profissionais aptos para tanto.

Sem medo de errar

Lembre-se de que nesta seção você deverá elaborar a segunda parte do parecer, que consiste na sua opinião legal em relação à legalidade da medida proposta no projeto de lei que trata da criação de um modelo público de autenticação de acesso à rede por meio do número de CPF do usuário. Tal medida criou uma polêmica muito grande com a ONG Defensores da Privacidade Online. Eles argumentam que tal medida violaria o direito constitucional à privacidade dos cidadãos e usuários da internet.

Após o estudo das disposições preliminares do Marco Civil da internet sobre os fundamentos, princípios e objetivos do uso da internet no Brasil, aliado ao estudo dos direitos e garantias dos usuários da rede, temos condições de emitirmos nossa opinião legal. Vamos lá?

QUESTÕES A SEREM RESPONDIDAS NO PARECER (CONT.)

- A MEDIDA CONSTANTE NO PROJETO DE LEI QUE PROPÕE A CRIAÇÃO DE UM MODELO PÚBLICO DE AUTENTICAÇÃO DE ACESSO À REDE POR MEIO DO NÚMERO DE CPF DO USUÁRIO PODE SER CONSIDERADA LEGAL, À LUZ DO MARCO CIVIL DA INTERNET?

Resposta: Primeiramente, podemos afirmar que uma medida dessa estirpe se classifica como verdadeiro incentivo à coleta maciça e desnecessária dos dados pessoais dos usuários da internet. Tal fato contraria os princípios, objetivos e direitos previstos no Marco Civil da Internet (MCI).

Primeiramente, temos que o MCI, em seu artigo 3º, adota como princípios a "proteção da privacidade" e a "proteção dos dados pessoais". Ora, a partir do momento que o Estado estabelece a obrigatoriedade da coleta do número de CPF por entidades privadas, sem qualquer consentimento do usuário, tal fato denota violação à privacidade desse usuário. Nesse sentido, o artigo 7º do MCI assegura como direito aos usuários o "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei" (BRASIL, 2014, [s.p.]). Assim, sem tal consentimento do usuário, a coleta de dados dessa natureza apresenta-se inviável. Igualmente, o artigo 4º define como um dos objetivos do uso da internet a promoção do direito de acesso à internet a todos. Tendo em vista que nem todas as pessoas possuem o Cadastro de Pessoa Física, tal fato violaria um dos objetivos do MCI, que é justamente garantir o acesso de todas as pessoas à internet.

Uma alternativa ao acesso via CPF seria, por exemplo, aumentar o período de guarda dos "logs", ou registros de atividades dos usuários na internet. Atualmente, as empresas devem guardá-los pelo período mínimo de um ano. Todavia, considerando a morosidade do Poder Judiciário, muitas vezes esse período apresenta-se insuficiente para a devida identificação de um usuário da rede.

Avançando na prática

A questão da "cláusula de foro"

Descrição da situação-problema

Você, na condição de advogado especialista em assuntos relacionados à regulação da internet no Brasil, foi procurado por uma empresa japonesa para prestar-lhe consultoria. Tal empresa é titular de um aplicativo que permite aos seus usuários obterem o ideograma japonês correspondente ao nome da pessoa. Além disso, o aplicativo apresenta os ideogramas relacionados aos signos dos usuários, utilizados comumente para tatuagens. Nos Termos de Uso do Site,

consta que qualquer avença relacionada ao uso do aplicativo deverá ser resolvida por meio de procedimento arbitral, sendo aplicável a lei japonesa para resolução de eventuais conflitos. Sua tarefa será analisar a legalidade da citada cláusula à luz do Marco Civil da Internet.

Resolução da situação-problema

A cláusula que define a lei japonesa como aplicável para resolução de conflitos é anulável, tendo em vista a norma contida no parágrafo único do artigo 8º do MCI, que estabelece que todas as cláusulas que "impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet" ou "em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil" são nulas. Dessa maneira, para ser válida, a cláusula descrita no enunciado deveria prever a adoção do foro brasileiro para a resolução de eventuais conflitos.

Faça valer a pena

1. O Marco Civil foi idealizado como um projeto de lei singular, não apenas por conta de seu conteúdo, mas também pelo seu processo de criação, debate e aprovação. O Marco Civil estabeleceu princípios, direitos e deveres para a rede no Brasil de forma articulada com os princípios da democracia.
Assinale a alternativa que apresenta um fundamento do Marco Civil da Internet, nos termos de seu artigo 2º.
a) Liberdade econômica.
b) Finalidade econômica da rede.
c) Reconhecimento da escala mundial da rede.
d) Defesa da concorrência.
e) Multilateralidade.

2. Em reportagem, foi noticiado que "clientes da operadora [...] com planos pré-pagos e os chamados 'controle' terão sua internet cortada após o fim da franquia de dados. A empresa abandona assim a oferta de internet com velocidade reduzida após a franquia e passa a esperar que o cliente contrate um pacote adicional de dados para continuar conectado" (Disponível em: <http://www.gazetadopovo.com.br/economia/operadoras-cortam-internet-apos-limite-da-franquia-eh84i11a1bdr5l3czqwdo01fy>. Acesso em: 31 mar. 2017).
A medida adotada pela operadora, referente ao corte da internet após fim da franquia de dados, tem o condão de violar qual dos direitos dos usuários elencados a seguir?

Assinale a única alternativa correta que responde ao questionamento.
a) Inviolabilidade da intimidade e da vida privada.
b) Não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização.
c) Manutenção da qualidade contratada da conexão à internet.
d) Inviolabilidade e sigilo do fluxo de suas comunicações pela internet.
e) Publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet.

3. O artigo 8º do Marco Civil da Internet estabelece que o exercício do direito de acesso à internet tem como condição a garantia do direito à privacidade e liberdade de expressão, sendo que eventuais cláusulas contratuais que violem tais direitos poderão ser consideradas nulas.
Assinale a alternativa que apresenta um exemplo de cláusula anulável à luz do artigo 8º do MCI:
a) Cláusula elegendo o foro brasileiro como competente para a resolução de controvérsias, nos casos de contratos de adesão decorrentes de serviços prestados no Brasil.
b) Cláusula que garante o sigilo de comunicações privadas efetuadas pela internet.
c) Cláusula que permita o tratamento de dados pessoais dos usuários sem seu consentimento expresso.
d) Cláusula que permita a remoção de conteúdos lícitos por estar contrária a determinada ideologia política.
e) Cláusula que estabeleça padrões técnicos de proteção de dados pessoais.

Seção 1.3

Neutralidade da rede

Diálogo aberto

Olá aluno! Nas seções anteriores estudamos como a internet vem sendo regulada, sobretudo em território brasileiro. Vimos que o Marco Civil da Internet representou um grande avanço legislativo nessa seara, estabelecendo fundamentos, princípios e objetivos ao uso da internet no Brasil. Entre esses princípios, um dos mais polêmicos certamente é o da neutralidade da rede, que é abordado sob diferentes pontos de vista. Nesse sentido, um dos tópicos mais debatidos diz respeito ao modelo *zero rating*, existindo aqueles que defendem que tal modelo de negócio viola o princípio da neutralidade da rede, conforme disposto no Marco Civil da Internet, e outros que afirmam que não existe tal violação, dependendo da maneira como os dados são discriminados.

Com foco nessa discussão, vamos relembrar nosso contexto de aprendizagem. Após tornar público seu projeto de lei, o senador "José da Telecom" contratou uma empresa para desenvolvimento de um aplicativo para smartphones que permite aos usuários dizerem se gostam ou não dessa iniciativa, bem como dar sua opinião sobre pontos específicos.

Como esse senador possui uma relação estreita com uma determinada empresa de telecomunicação, ambos fizeram um acordo para que o aplicativo fosse oferecido aos clientes dessa operadora na modalidade *zero rating*, ou seja, sem descontar dados do pacote contratado. Esse modelo de acordo é compatível com o Marco Civil? Tal análise deverá constar na última parte de seu produto, o parecer jurídico contendo a opinião legal de um consultor especialista, analisando a viabilidade de um projeto de lei que visa regular a internet brasileira. Para a resolução da questão, iremos nos aprofundar no conceito de neutralidade da rede, seus aspectos técnicos e reflexos econômicos.

Não pode faltar

Conforme vimos na seção anterior, toda a sociedade civil foi convidada a participar do debate em torno da elaboração do Marco

Civil da Internet, o que gerou amplas discussões sobre sua construção. Uma das questões mais controversas foi, definitivamente, aquela relacionada à neutralidade da rede.

Assimile

A neutralidade da rede foi concebida como verdadeiro princípio para o uso da internet no Brasil (art. 3º, inciso IV da Lei nº 12.965/2014), sendo também um princípio de arquitetura da rede, que endereça aos provedores de acesso o dever de tratar os pacotes de dados que trafegam em suas redes de forma isonômica, não os discriminando em razão de seu conteúdo ou origem (RAMOS, 2015).

Vamos começar apresentando a você alguns aspectos técnicos sobre a neutralidade da rede. Apesar de ser tratada especificamente no Marco Civil da Internet, a neutralidade encontra guarida também no aspecto infralegal, com a Resolução da Anatel nº 614, de 28 de maio de 2013, que aprovou o Regulamento do Serviço de Comunicação Multimídia (SCM), determinando, em seu artigo 75, a obrigação de respeito à neutralidade pelas operadoras responsáveis por agregar à rede de serviço telefônico as funcionalidades que permitem o tráfego de dados em banda larga. Cite-se, ainda, o seguinte trecho da Resolução do Comitê Gestor da Internet nº 003 (CGI.br/RES/003) de 2009: "filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento" (COMITÊ GESTOR DA INTERNET, 2009a, [s,p.].

A Resolução do CGI.br citada ilustra bem os fundamentos que embasaram a norma contida no artigo 9º do Marco Civil da Internet, que assim dispõe:

> **Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.**
> **§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:**

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações;
II - priorização de serviços de emergência.
§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no caput deve:
I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei no 10.406, de 10 de janeiro de 2002 - Código Civil;
II - agir com proporcionalidade, transparência e isonomia;
III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e
IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.
§ 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo. (BRASIL, 2014, [s.p.])

Há pelo menos três formas de discriminar um conteúdo ou aplicação específica na internet: I) bloqueando; II) reduzindo sua velocidade; e III) cobrando um valor diferenciado pelo acesso àquele conteúdo ou aplicação. O bloqueio de conteúdos é muito comum em países mais rígidos, marcados pelo controle censório da internet (ex.: China e Turquia). A redução de velocidade ocorre quando determinado aplicativo específico não é carregado na mesma velocidade dos demais. Isso pode ocorrer por diversas razões: para diminuir a qualidade de um serviço concorrente aos serviços da telefonia tradicional (ex.: VoIP e serviços de mensagens OTT); para favorecer o acesso dos usuários a determinado parceiro comercial; para reduzir o consumo de banda em aplicações pesadas (ex.: *streaming* de vídeos, como YouTube e Netflix); ou mesmo impedir o acesso a serviços que potencialmente violam direitos de propriedade intelectual de empresas parceiras dos provedores de acesso (ex.: protocolos Bittorrent) (RAMOS, 2015).

Ademais, os provedores de acesso podem discriminar também cobrando diferentes preços por serviços ou aplicações. Essa diferenciação pode vir a partir da cobrança de uma taxa a mais para acesso a determinados conteúdos, semelhante ao que

ocorre atualmente nos modelos de TV por assinatura. Por fim, os provedores podem dar gratuidade no acesso a alguns aplicativos, em razão de arranjos comerciais, algo que pode danificar um cenário competitivo entre aplicações semelhantes (e que estudaremos com mais detalhes posteriormente).

Em que pese o Marco Civil da Internet garantir a neutralidade da rede como princípio de arquitetura e uso da internet, cumpre trazer à tona o posicionamento dos especialistas técnicos em Tecnologia da Informação, que são unânimes em dizer que não pode haver uma neutralidade absoluta, por questões de segurança da rede. A principal exceção à neutralidade reconhecida por esses especialistas diz respeito ao bloqueio de caminhos que sejam considerados portas de entrada para o envio de vírus e spam. A título de exemplificação, podemos citar o caso da chamada "Porta 25" no Brasil.

A "Porta 25" é uma entrada de tráfego que passou a ser massivamente utilizada por *spammers* e, portanto, passou a representar uma porta de entrada de mensagens indesejáveis aos usuários da rede. O CGI.br adotou uma Resolução para o gerenciamento do tráfego vindo por essa porta (COMITÊ GESTOR DA INTERNET, 2009b).

Assim, o bloqueio de uma porta de entrada, de forma a impedir ataques que causem a instabilidade da rede por excesso de tráfego malicioso, torna-se necessário quando se detecta o uso dessa porta predominantemente por agentes mal-intencionados, sendo certo que práticas dessa natureza somente seriam possíveis se comprovada a inexistência de prejuízo para a efetiva entrega de pacotes para uso de aplicações por usuários pela via de outras portas de acesso à rede.

Além dos ataques à rede, o Marco Civil da Internet, em sua exposição de motivos, menciona uma possível discriminação técnica de tráfego entre tipos de serviços. Os provedores devem dar preferência à passagem integral de pacotes contínuos de uma determinada aplicação da internet, de forma unificada e contínua, de modo a não prejudicar a percepção de qualidade pelo usuário. Trata-se do caso de serviços que dependem da passagem sequencial de dados, sem interrupções, como VoIP (*Voice over Internet Protocol* ou Voz sobre Protocolo de Internet) e vídeos. Por outro lado, serviços que não dependem da entrega contínua de pacotes, como e-mails, não se enquadrariam nessa exceção.

Ato contínuo, o texto legal contido no artigo 9º do Marco Civil da Internet foi minucioso ao estabelecer as situações nas quais são admitidas exceções à neutralidade: I) quando houver requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e II) a priorização de serviços de emergência. Ambas as hipóteses de degradação foram regulamentadas pelo Decreto nº 8.771 de 2016. Em relação à primeira hipótese de degradação, o decreto assim dispõe:

> Art. 5º Os requisitos técnicos indispensáveis à prestação adequada de serviços e aplicações devem ser observados pelo responsável de atividades de transmissão, de comutação ou de roteamento, no âmbito de sua respectiva rede, e têm como objetivo manter sua estabilidade, segurança, integridade e funcionalidade.
> § 1º Os requisitos técnicos indispensáveis apontados no caput são aqueles decorrentes de:
> I - tratamento de questões de segurança de redes, tais como restrição ao envio de mensagens em massa (spam) e controle de ataques de negação de serviço; e
> II - tratamento de situações excepcionais de congestionamento de redes, tais como rotas alternativas em casos de interrupções da rota principal e em situações de emergência.
> § 2º A Agência Nacional de Telecomunicações – Anatel atuará na fiscalização e na apuração de infrações quanto aos requisitos técnicos elencados neste artigo, consideradas as diretrizes estabelecidas pelo Comitê Gestor da Internet – CGI.br. (BRASIL, 2016, [s.p.])

Perceba que a norma mencionada veio a regular justamente as situações anteriormente narradas, como o gerenciamento em caso de ataques à rede, bem como a questão do gerenciamento de tráfego em caso de congestionamento, de modo a garantir a qualidade da conexão dos usuários da internet.

Por sua vez, a segunda hipótese de discriminação, referente à priorização dos serviços de emergência, foi tratada no artigo 8º do aludido decreto:

> Art. 8º A degradação ou a discriminação decorrente da priorização de serviços de emergência somente poderá decorrer de:

> I - comunicações destinadas aos prestadores dos serviços de emergência, ou comunicação entre eles, conforme previsto na regulamentação da Agência Nacional de Telecomunicações – Anatel; ou
> II - comunicações necessárias para informar a população em situações de risco de desastre, de emergência ou de estado de calamidade pública.
> Parágrafo único. A transmissão de dados nos casos elencados neste artigo será gratuita. (BRASIL, 2016, [s.p.])

Exemplificando

Um exemplo de uma aplicação que se enquadra na hipótese prevista no artigo supracitado trata-se do aplicativo "0800 Saúde", criado pelo Governo Federal, que traz informações de utilidade pública sobre o vírus Zika, como as causas da doença e sua relação com casos de microcefalia em recém-nascidos. O aplicativo também tem orientações sobre como combater o mosquito Aedes aegypti, transmissor da zika, da dengue e da chikungunya.

Fica clara a posição do legislador em permitir a discriminação dos pacotes de dados apenas em situações emergenciais e, sobretudo, de interesse público, ou ainda, que atenda aos "requisitos técnicos indispensáveis" (BRASIL, 2016, [s.p.]).

Ademais, o Decreto nº 8.771/16, em seu art. 9º, ainda vedou:

> [...] condutas unilaterais ou acordos entre o responsável pela transmissão, pela comutação ou pelo roteamento e os provedores de aplicação que:
> I - comprometam o caráter público e irrestrito do acesso à internet e os fundamentos, os princípios e os objetivos do uso da internet no País;
> II - priorizem pacotes de dados em razão de arranjos comerciais, ou;
> III - privilegiem aplicações ofertadas pelo próprio responsável pela transmissão, pela comutação ou pelo roteamento ou por empresas integrantes de seu grupo econômico. (BRASIL, 2016, art. 9º)

E vedou ainda, em seu art. 10, que:

> **[...] as ofertas comerciais e os modelos de cobrança de acesso à internet devem preservar uma internet única, de natureza aberta, plural e diversa, compreendida como um meio para a promoção do desenvolvimento humano, econômico, social e cultural, contribuindo para a construção de uma sociedade inclusiva e não discriminatória. (BRASIL, 2016)**

Entre tais vedações, a mais polêmica certamente diz respeito ao inciso II do artigo 9º ("acordos que priorizem pacotes de dados em razão de arranjos comerciais"). Isso porque tal vedação abarcaria os chamados aplicativos *zero rating*.

O *zero rating* é uma prática realizada por prestadoras de serviços de telecomunicações que consiste em aplicar um "preço zero" para o tráfego de dados móveis associado a uma aplicação ou classe de aplicações em particular, implicando na não contagem desse tráfego para efeitos de uma franquia de dados eventualmente aplicada ao acesso à internet contratado (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, 2016).

A título de exemplo de modelos *zero rating* no Brasil, podemos citar o caso de algumas operadoras brasileiras que possuem planos nos quais o tráfego de dados de alguns aplicativos – como o WhatsApp ou Facebook – não contam para o consumo mensal da franquia.

O *zero rating* pode ser entendido como uma série de estratégias comerciais. A seguir, exemplificamos algumas:

a) Tarifação zero por escolha da própria prestadora: a prestadora de serviço de telecomunicações elege, segundo critérios pautados em uma decisão interna, determinados conteúdos ou aplicações que, quando acessados pelo usuário, não gerarão qualquer tipo de custo;

b) Tarifação zero para aplicações ou serviços de emergência: o acesso a aplicações ou serviços de utilidade pública específicos não são cobrados do usuário;

c) Dados patrocinados: nesse caso, o patrocinador arca com os custos dos dados trafegados pelo usuário final quando destinarem-se ao acesso a website específico ou utilização de determinado aplicativo;

d) Gerenciamento de dados: consiste no gerenciamento de tráfego direcionado a provedores de conteúdo, a fim de que estes se utilizem de períodos de menor demanda de tráfego, os quais são

consequentemente mais baratos, para entrega de seu conteúdo de forma mais eficiente;

e) Dados como recompensa: ocorre quando uma marca, desejando engajar determinado consumidor, lhe oferece a possibilidade de acesso a dados móveis, com custo zero, como recompensa por assistir um vídeo específico, baixar certo aplicativo ou realizar determinada ação desejada;

f) Publicidade direcionada: nesse caso, direciona-se a publicidade de determinado produto àqueles consumidores que, segundo informações de seu acesso, efetivamente têm interesse. Nesse caso, o usuário que baixar o aplicativo ou acessar o conteúdo desejado não pagará por tê-lo feito;

g) Dados corporativos: permite que determinada instituição arque apenas com acesso a dados corporativos. Os dados pessoais serão custeados pelo próprio funcionário.

Reflita

A possibilidade de realização de acordos envolvendo aplicações *zero rating* entre operadoras de telefonia e desenvolvedores é algo longe de ser pacífico, existindo argumentos tanto a favor dessa possibilidade quanto contra tal prática, conforme veremos. Em sua opinião, tal prática viola ou não o princípio da neutralidade da rede?

A princípio, não nos parece correto o enquadramento do *zero rating* nas hipóteses de quebra da neutralidade estabelecidas pelo MCI e pelo Decreto nº 8.771/2016, uma vez que não decorre de questões de natureza técnica e nem de implicações emergenciais. Trata-se de verdadeiro modelo de negócio advindo de arranjos comerciais. Para os defensores da possibilidade de acordos *zero rating*, tal prática não implicaria necessariamente em violação ao princípio da neutralidade da rede, uma vez que garantiria a possibilidade de acesso à internet para os usuários, mesmo após o esgotamento de sua franquia de dados, o que geraria inclusão digital na sociedade.

Por outro lado, aqueles que defendem que esta prática fere o MCI argumentam que:

> **[...] restringir o alcance da garantia da neutralidade à aspectos exclusivamente técnicos, expurgando reflexões mais amplas e de natureza jurídica, significa ignorar a realidade de que os agentes econômicos que atuam na**

> cadeia da Internet estão cada vez mais concentrados, prestando os serviços de forma vertical, associando-se para explorar a infraestrutura de telecomunicações e comercializar serviços de acesso à Internet e fornecimento de aplicações e conteúdos, com o objetivo de impedir a concorrência efetiva e manter altos preços de forma cartelizada, colocando em risco o caráter democrático da rede. (LEFÈVRE, 2015, [s.p.])

Pesquise mais

Recentemente, a Anatel se manifestou no sentido de que acordos comerciais envolvendo aplicações zero rating não possuem caráter anticoncorrencial, ou seja, não impedem a plena concorrência. A manifestação foi feita a partir de uma consulta solicitada pelo Conselho Administrativo de Defesa Econômica (CADE) para auxiliar na instrução do Inquérito Administrativo nº 08700.004314/2016-71, instaurado a partir de representação do Ministério Público Federal junto ao CADE, em face de Claro S.A., Tim Celular S.A., Oi Móvel S.A. e Telefonica Brasil S.A., sob a alegação de que as representadas estariam incorrendo em condutas anticompetitivas, consubstanciadas no tratamento discriminatório entre os diversos conteúdos e aplicativos acessados por meio de suas redes (zero rating). O inteiro teor da análise está disponível em: <https://sei.anatel.gov.br/sei/publicacoes/controlador_publicacoes.php?acao=publicacao_visualizar&id_publicacao_legado=&id_documento=1100301&id_orgao_publicacao=0> (acesso em: 11 abr. 2017).

Ademais, vimos a importância que o estabelecimento de uma regra determinando a neutralidade da rede tem sobre a economia do país. Em razão disso, não é de se surpreender que diferentes lados, com diferentes pontos de vista, tentem fazer prevalecer sua vontade.

Sem medo de errar

Até o momento, estudamos como foi o processo evolutivo do Direito Eletrônico e consequentemente da regulação do ambiente digital, principalmente em território brasileiro. Vimos também que o Marco Civil da nternet foi muito importante para acabar com o antiquado conceito de que a internet é "terra sem lei". O MCI estabeleceu diversos princípios e garantias para o uso da rede no Brasil. Nesta seção, aprofundamos nossos estudos sobre um desses princípios, qual seja, a neutralidade da rede.

Demonstrados os aspectos técnicos e jurídicos da neutralidade da rede, vamos resolver a situação-problema proposta?

Relembre que o senador "José da Telecom" contratou uma empresa para desenvolvimento de um aplicativo para smartphones que permite aos usuários dizerem se gostam de um projeto de lei, especificamente o criado pelo senador conforme descrito ao longo da unidade, bem como dar sua opinião sobre pontos específicos do projeto. O senador e uma determinada empresa de telecomunicação fizeram um acordo para que o aplicativo fosse oferecido aos clientes dessa operadora na modalidade *zero rating*, ou seja, sem descontar dados do pacote de franquia contratado. Esse modelo de acordo é compatível com o Marco Civil? Para responder esse questionamento, iremos precisar retomar o conceito de neutralidade da rede e suas exceções legais e técnicas. Esta será a última parte de seu produto, o parecer jurídico contendo a opinião legal de um consultor especialista, analisando a viabilidade de um projeto de lei que visa regular a internet brasileira.

Vamos finalizar nosso parecer jurídico?

APLICATIVOS ZERO RATING E O PRINCÍPIO DA NEUTRALIDADE DA REDE

- Parte Final do Parecer: Eventual acordo comercial que privilegia determinada aplicação, oferecida na modalidade zero rating, viola o princípio da neutralidade da rede, conforme previsto no Marco Civil da Internet e no Decreto nº 8.771/2016?

Antes de adentrarmos na análise concreta do caso, é importante definirmos o conceito de neutralidade da rede. Trata-se de verdadeiro princípio para o uso da internet no Brasil, nos termos do art. 3º, inciso IV da Lei nº 12.965/2014, sendo também um princípio de arquitetura da rede, que endereça aos provedores de acesso o dever de tratar os pacotes de dados que trafegam em suas redes de forma isonômica, não os discriminando em razão de seu conteúdo ou origem.

A neutralidade da rede está prevista especificamente no artigo 9º do Marco Civil da Internet, bem como no artigo 5º do Decreto nº 8.771 de 2016, que regulamentou o MCI. Ambas as normas trazem a previsão de que a neutralidade deve ser observada, sendo vedada a discriminação dos dados trafegados, exceto: I) quando houver requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e II) a priorização de serviços de emergência.

Assim, para que um provedor de acesso quebre a regra da neutralidade, deverá observar essas duas situações. O aplicativo idealizado para o senador, com objetivo de medir a popularidade de um projeto de lei de sua iniciativa, a princípio, não se enquadra em nenhuma das hipóteses de exceção da neutralidade da rede. Nesse sentido, a eventual descriminação do tráfego de dados de modo a privilegiar citada aplicação não compromete a prestação adequada dos serviços disponíveis na internet, que seria possível somente em casos como o bloqueio da "Porta 25" ou o privilégio de serviços que demandam tráfego contínuo de dados, como VoIP. Igualmente, não nos parece que o aplicativo proposto possa ser enquadrado como um serviço de emergência.

Ademais, o Decreto nº 8.771/16 ainda vedou:

> [...] condutas unilaterais ou acordos entre o responsável pela transmissão, pela comutação ou pelo roteamento e os provedores de aplicação que: I) comprometam o caráter público e irrestrito do acesso à internet e os fundamentos, os princípios e os objetivos do uso da internet no País; II) priorizem pacotes de dados em razão de arranjos comerciais, ou; III) privilegiem aplicações ofertadas pelo próprio responsável pela transmissão, pela comutação ou pelo roteamento ou por empresas integrantes de seu grupo econômico. (BRASIL, 2016, [s.p.])

E ainda, que:

> [...] as ofertas comerciais e os modelos de cobrança de acesso à internet devem preservar uma internet única, de natureza aberta, plural e diversa, compreendida como um meio para a promoção do desenvolvimento humano, econômico, social e cultural, contribuindo para a construção de uma sociedade inclusiva e não discriminatória. (BRASIL, 2016, [s.p.])

Dessa maneira, podemos dizer que o aplicativo idealizado pelo nosso Senador viola a neutralidade da rede, não sendo possível seu oferecimento na modalidade *zero rating*.

Avançando na prática

Bloqueio de aplicações e o princípio da neutralidade da rede

Descrição da situação-problema

Considere a seguinte situação hipotética: Após uma polêmica reportagem publicada em um site de notícias internacional criticando

o Presidente da República, acusando-o de corrupção, o governo federal emitiu um decreto determinando que os provedores de acesso à internet brasileiros proibissem os acessos de seus clientes e usuários ao conteúdo disponibilizado no site de notícias. Você, na condição de advogado de um desses provedores de acesso, foi consultado para saber se tal medida é legítima e se ela está em conformidade com o Marco Civil da Internet.

Resolução da situação-problema

O Marco Civil da Internet foi criado como instrumento para garantir os direitos básicos dos usuários da rede e para preservar uma internet livre e aberta. Para tanto, o MCI estabeleceu como um de seus princípios a chamada "neutralidade da rede", que por sua vez endereça aos provedores de acesso o dever de tratar os pacotes de dados que trafegam em suas redes de forma isonômica, não os discriminando em razão de seu conteúdo ou origem.

Nesse sentido, lembre-se de que existem pelo menos três formas de discriminar um conteúdo ou aplicação específica na internet: I) bloqueando; II) reduzindo sua velocidade; e III) cobrando um valor diferenciado pelo acesso àquele conteúdo ou aplicação. O bloqueio de conteúdos é muito comum em países mais rígidos, marcados pelo controle censório da internet (ex.: China e Turquia). A redução de velocidade ocorre quando determinado aplicativo específico não é carregado na mesma velocidade dos demais. Isso pode ocorrer por diversas razões: para diminuir a qualidade de um serviço concorrente aos serviços da telefonia tradicional (ex.: VoIP e serviços de mensagens OTT); para favorecer o acesso dos usuários a determinado parceiro comercial; para reduzir o consumo de banda em aplicações pesadas (ex.: *streaming* de vídeos, como YouTube e Netflix); ou mesmo impedir o acesso a serviços que potencialmente violam direitos de propriedade intelectual de empresas parceiras dos provedores de acesso (ex.: protocolos Bittorrent) (RAMOS, 2015, p. 138).

Dessa maneira, qualquer lei ou decisão que vise ao bloqueio de determinada aplicação ou conteúdo, conforme descrito na situação-problema, será ilegítima e contrária aos princípios estabelecidos no Marco Civil da Internet, sobretudo o da neutralidade da rede.

Faça valer a pena

1. A neutralidade da rede está prevista especificamente no artigo 9º do Marco Civil da Internet, bem como no artigo 5º do Decreto nº 8.771 de 2016, que regulamentou o MCI. Ambas as normas trazem a previsão de

que a neutralidade deve ser observada, sendo vedada a discriminação dos dados trafegados, exceto nas hipóteses legais, previstas em lei.
Assinale a única alternativa correta que apresenta uma exceção válida ao princípio da neutralidade da rede:
a) Cobrança de valores diferenciados para acesso a aplicações de *streaming* de vídeos.
b) Bloqueio de aplicações em razão de seu conteúdo.
c) Privilégio de tráfego de dados em razão de arranjos comerciais.
d) Degradação do tráfego de dados de aplicações concorrentes aos provedores de acesso.
e) Bloqueio de caminhos que sejam considerados portas de entrada para o envio de vírus e spam.

2. Além dos ataques à rede, o Marco Civil da Internet, em sua exposição de motivos, menciona uma possível discriminação técnica de tráfego entre tipos de serviços. Os provedores devem dar preferência à passagem integral de pacotes contínuos de uma determinada aplicação da internet, de forma unificada e contínua, de modo a não prejudicar a percepção de qualidade pelo usuário.
Assinale a única correta alternativa que apresenta um exemplo de serviço que se encaixa na discriminação técnica de tráfego de dados narrada:
a) Desenvolvimento de linguagens.
b) *Streaming* de vídeos.
c) Banco de dados.
d) SQL.
e) Sistemas de Informação Gerencial.

3. O *zero rating* é uma prática realizada por prestadoras de serviços de telecomunicações que consiste em aplicar um "preço zero" para o tráfego de dados móveis associado a uma aplicação ou classe de aplicações em particular, implicando na não contagem desse tráfego para efeitos de uma franquia de dados eventualmente aplicada ao acesso à internet contratado. O *zero rating* pode ser entendido como uma série de estratégias comerciais.
Assinale a alternativa que apresenta um exemplo válido de estratégia comercial que configura a prática de *zero rating*:
a) Tarifação zero para aplicações ou serviços de emergência.
b) Dados como ferramenta de publicidade.
c) Dados como venda.
d) Bloqueio de aplicações desenvolvidas pela própria prestadora.
e) Tarifação zero por escolha de outra prestadora.

Referências

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. Análise nº 100/2016/SEI/AD. 9 nov. 2016. Disponível em: <https://sei.anatel.gov.br/sei/publicacoes/controlador_publicacoes.php?acao=publicacao_visualizar&id_publicacao_legado=&id_documento=1100301&id_orgao_publicacao=0>. Acesso em: 11 abr. 2017.

BARLOW, John Perry. Declaração de independência do ciberespaço. **DHnet**, [s.d.]. Disponível em: <http://www.dhnet.org.br/ciber/textos/barlow.htm>. Acesso em: 17 abr. 2017.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 5 abr. 2017.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 6 nov. 2018.

_____. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014. 11 maio 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 5 abr. 2017

COMITÊ GESTOR DA INTERNET. Resolução CGI.br/RES/2009/03/P: princípios para a governança e uso da internet no Brasil. **CGI.br**, 2009a. Disponível em: <https://www.cgi.br/resolucoes/documento/2009/003>. Acesso em: 24 abr. 2017.

_____. Resolução CGI.br/RES/2009/02/P: recomendação para adoção de gerência de Porta 25 em redes de caráter residencial. **CGI.br**, 2009b. Disponível em: <https://www.cgi.br/resolucoes/documento/2009/002> . Acesso em: 24 abr. 2017.

DE LUCA, Cristina. Bloqueio do Whatsapp viola o Marco Civil e a Constituição, afirma Ronaldo Lemos. **IDGNOW!**, 17 dez. 2015. Disponível em: <http://idgnow.com.br/mobilidade/2015/12/17/bloqueio-do-whatsapp-viola-o-marco-civil-e-a-constituicao-afirma-ronaldo-lemos/>. Acesso em: 17 abr. 2017.

DE LUCCA, Newton. Marco Civil da Internet: uma visão panorâmica dos principais aspectos relativos às suas disposições preliminares. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito e internet III**. São Paulo: Quartier Latin, 2015. Tomo I: Marco Civil da Internet (Lei n. 12.965/2014).

_____; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito e Internet III**. São Paulo: Quartier Latin, 2015. Tomo I: Marco Civil da Internet (Lei n. 12.965/2014).

GOLDMAN, Eric. The third wave of Internet exceptionalism. **Santa Clara Magazine**, 2008.

LEFÈVRE, Flávia. Zero-rating, planos de serviços limitados e o direito de acesso à internet. **poliTICs**, ago. 2015. Disponível em: <https://www.politics.org.br/edicoes/zero-rating-planos-de-servi%C3%A7o-limitados-e-o-direito-de-acesso-%C3%A0-internet>. Acesso em: 17 abr. 2017.

LEINER, Barry M. et al. **A brief history os the internet**. 1997. Disponível em: <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet>. Acesso em: 14 mar. 2017.

LEMOS, Ronaldo. Uma breve história da criação do Marco Civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito e internet III.** São Paulo: Quartier Latin, 2015. Tomo I: Marco Civil da Internet (Lei n. 12.965/2014).

_____; SOUZA, Carlos Affonso. **Marco Civil da Internet**: construção e aplicação. Juiz de Fora: Editar Editora Associada Ltda., 2016. Disponível em: <https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf>. Acesso em: 5 abr. 2017.

LESSIG, Lawrence. **Code and other laws of cyberspace**. Nova York: Basic Books, 1999.

PINHEIRO, Patrícia Peck. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2016.

RAMOS, Pedro Henrique Soares. O Marco Civil e a importância da neutralidade da rede: evidências empíricas no Brasil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito e internet III**. São Paulo: Quartier Latin, 2015. Tomo I: Marco Civil da Internet (Lei n. 12.965/2014).

ROHRMANN, Carlos Alberto. **Curso de Direito Virtual**. Belo Horizonte: Del Rey, 2005.

WU, Timothy S. Cyberspace sovereignty? The internet and the international system. **Harvard Journal of Law and Technology**, n. 10, p. 647, 1997.

Direitos da personalidade na internet e responsabilidade civil

Convite ao estudo

Conforme estudamos na unidade anterior, a popularização da rede mundial de computadores trouxe consigo o aparecimento de diversas situações que desafiavam o contexto jurídico da época. Isso levou à necessidade de se criar um ramo "especial" dentro do próprio Direito que fosse capaz de lidar com essas novas situações ocorridas dentro do ambiente eletrônico. Surgia, assim, em meados da década de 1990, o Direito Eletrônico, também chamado de Direito Digital ou Direito da Informática. Logo, os primeiros estudos acerca do tema começaram a ser publicados no meio acadêmico. Igualmente, as primeiras legislações com objetivo específico de regular o espaço virtual começaram a aparecer. Entretanto, somente no ano de 2014 é que o Brasil conseguiu aprovar uma lei específica e contundente para assegurar os direitos dos usuários da internet no Brasil, qual seja, o Marco Civil da Internet.

O referido diploma legal serve como verdadeira bússola para a resolução de problemas jurídicos na rede, ao passo que criou normas específicas para determinadas situações, bem como estabeleceu princípios e garantias básicas para a proteção dos citados usuários. Tais princípios reiteram direitos constitucionalmente garantidos, tais como os direitos da personalidade dos usuários, os quais serão estudados nesta Unidade 2.

Como dito anteriormente, o Marco Civil da Internet tratou com destaque os direitos da personalidade, contextualizando-os dentro da Sociedade da Informação. Observe que a liberdade de expressão e a privacidade dos usuários apresentam-se como pilares na formação de um corpo normativo aplicado ao uso da internet em território brasileiro. Consequentemente,

eventuais violações desses e de outros direitos acarretam na responsabilização civil do agente causador. Simultaneamente, tal responsabilização foi ocasionalmente limitada aos provedores de aplicação justamente com objetivo de garantir efetividade a tais direitos da personalidade. Todavia, ocorrem situações em que dois ou mais desses direitos colidem entre si. Assim, a proposta da unidade é estudar os direitos da personalidade dentro do contexto da Sociedade da Informação e do Marco Civil da Internet, bem como seus limites e hipóteses de colidência, além das regras sobre a responsabilidade civil daqueles que violam tais direitos.

Para tanto, iremos considerar o seguinte contexto de aprendizagem: em razão do trabalho prévio elaborado para a Comissão de Ciência e Tecnologia do Senado, o deputado "Polêmico Oliveira" procurou você para auxiliá-lo em um caso particular. O deputado vem tendo sua honra e imagem atacadas constantemente pelo blogueiro "João Falastrão". Em seu blog pessoal (www.joaofalastrao.com.br), que conta com mais de 50 mil seguidores, João realiza críticas vorazes à política feita pelo deputado. De maneira geral, as críticas são de cunho político. Todavia, em determinada ocasião, João publicou um conteúdo, muito difundido nas redes sociais, acusando o deputado Polêmico de corrupção passiva, conforme previsto no Código Penal. Você, na condição de advogado do deputado Polêmico Oliveira, deverá tomar as medidas jurídicas cabíveis para remover o citado conteúdo do blog de João Falastrão.

Nesse sentido, iremos elaborar uma notificação extrajudicial, bem como uma petição inicial, com o objetivo de remover o conteúdo ilícito publicado no blog. As referidas peças serão elaboradas com a contribuição de cada situação-problema (SP). Na SP.1, você deverá analisar os direitos da personalidade das partes. Na SP.2, você deverá elaborar uma petição inicial, requerendo a remoção dos conteúdos ofensivos. Na SP.3, você finalizará sua petição inicial, analisando a responsabilidade civil dos provedores de aplicação por conteúdos gerados por terceiro.

No intuito de resolver os problemas advindos do contexto de aprendizagem, estudaremos, na Seção 2.1, o conceito de direito

da personalidade, sua contextualização perante o Marco Civil da Internet e a resolução de conflitos em caso de colidência entre tais direitos. Já na Seção 2.2, estudaremos a proteção garantida à privacidade e aos dados pessoais dos usuários, bem como sua liberdade de expressão e os limites dessa proteção. Por fim, na Seção 2.3, iremos analisar a responsabilidade civil dos provedores de internet, além de seu dever de guarda de registros de aplicação e conexão. Vamos aos trabalhos?

Seção 2.1

Direitos da personalidade na internet

Diálogo aberto

O primeiro passo para a remoção do conteúdo ofensivo publicado no blog é alertar o autor, no caso o blogueiro João, de que o conteúdo publicado possivelmente viola direitos fundamentais do seu cliente, o deputado Polêmico. Nos casos envolvendo esse tipo de incidente digital, quanto mais tempo o conteúdo ficar on-line, maiores serão os danos causados à vítima. Nesse sentido, é comum o advogado optar por soluções extrajudiciais, sobretudo em razão da celeridade. Assim, seguiremos esse caminho, que se trata de uma primeira etapa no procedimento de tentativa de remoção de conteúdos ilícitos da internet. Para tanto, redija uma breve **notificação extrajudicial**, alertando o blogueiro sobre os direitos do deputado que estão sendo violados, bem como as medidas que deverão ser tomadas de modo a evitar eventual interposição de medida judicial.

Ao longo da seção, iremos analisar o conceito de direito da personalidade e sua aplicação dentro do contexto da rede mundial de computadores. Inevitavelmente, iremos nos deparar com situações de conflitos entre tais direitos; portanto, apresenta-se imprescindível o estudo de métodos resolutivos desse tipo de conflito. Especificamente, iremos estudar o princípio da proporcionalidade como ferramenta para solução dessa celeuma.

Vamos lá?

Não pode faltar

Como provavelmente você deve ter estudado no início da matéria de Direito Civil, especificamente na parte de Pessoas e Bens, a doutrina clássica conceitua os direitos da personalidade como aqueles a par dos direitos economicamente apreciáveis, mas não menos valiosos, merecedores de amparo e proteção da ordem jurídica. Tais direitos seriam atinentes à própria natureza humana.

Assimile

Os direitos da personalidade são os direitos de cada pessoa de defender o que lhe é próprio, como a vida, identidade, liberdade (informativa, de expressão e de pensamento), privacidade (inclusive proteção de dados pessoais), honra, opção sexual, integridade, imagem, valendo-se de ação judicial em caso de eventual ofensa ou violação (PEREIRA, 2007).

Partindo-se de um viés mais positivista, a Constituição Federal de 1988 enuncia direitos e garantias individuais e coletivos, que o legislador tem o dever de proteger e assegurar. Nesse sentido, destaca-se o princípio da dignidade da pessoa humana (art. 1º, III) como uma cláusula geral de tutela da personalidade.

Exemplificando

A "dignidade da pessoa humana" serve como verdadeiro corolário para outros direitos intrínsecos à personalidade, tais como privacidade, honra, imagem e liberdade de expressão. Trata-se de um valor fundamental que orienta e abarca a construção desses e de outros direitos. Daí dizermos que se trata de "cláusula geral" de tutela da personalidade.

Quando tratamos dos direitos da personalidade, cabe ressaltar que não constituem apenas "um direito", sendo equivocada qualquer afirmação no sentido de que o homem tem "direito à personalidade". Ora, a personalidade é o ponto de apoio de outros direitos e obrigações, ou seja, dela se irradiam diversos direitos. A Constituição Federal de 1988 declarou que são invioláveis a intimidade, a vida privada, a honra, a imagem das pessoas, assegurando o direito à indenização pelo dano moral ou material decorrente de sua violação (art. 5º, X).

Dentro de uma sistemática organizacional, os direitos da personalidade distribuem-se em duas categorias gerais: adquiridos e inatos. Os adquiridos existem nos termos e na extensão da disciplina do direito. Por outro lado, os inatos se sobrepõem a qualquer condição legislativa, sendo irrenunciáveis, intransmissíveis e imprescritíveis.

Assim, ocorrendo lesão ou ameaça contra qualquer direito da personalidade, o titular possui legitimidade para buscar a devida reparação, a ser avaliada com obediência aos critérios genéricos destinados à sua estimativa, independentemente de não serem dotados de patrimonialidade.

Em linhas gerais, os direitos da personalidade envolvem o direito à vida, à liberdade, ao próprio corpo, à incolumidade física, à proteção da intimidade, à integridade moral, à preservação da própria imagem, nome, às obras de criação do indivíduo e tudo mais que seja digno de proteção, amparo e defesa na ordem jurídica (PEREIRA, 2007).

Feitas tais considerações acerca dos direitos da personalidade e sua proteção, faz-se necessária uma reflexão mais profunda, levando-se em consideração as diversas aplicações de internet existentes, "que potencializaram todos os atos da vida particular e profissional de quem as utiliza, como maneira explícita de mudança de paradigma na manifestação dos direitos da personalidade" (HAIKAL, 2017, [s.p]).

Uma vez que os usuários de internet praticam os mais diversos atos cotidianos da vida por meio da rede mundial de computadores, é natural que exista a ampliação da projeção da personalidade de quem executa determinadas ações nesses ambientes digitais, haja vista não se limitarem mais ao meio físico, mas de recursos que, além de encurtarem distâncias, fazem com que um ato simplório reverbere para milhões de outras pessoas em questão de segundos.

Você provavelmente já reclamou de algum chefe, professor, político nas redes sociais. Caso negativo, pelo menos deve conhecer alguém que já fez isso. Pois então. Há uma grande chance de essa reclamação ter excedido o limite da liberdade de expressão, de modo a ofender um direto alheio, tal como a honra e imagem. Devemos estar sempre muito atentos a esse tipo de conduta, pois as mesmas regras que valem para o meio físico valem para o meio digital. Inclusive, o potencial dano causado no meio digital é até maior, pois alcança muito mais pessoas.

A partir do cenário de garantias estabelecido pelo ordenamento jurídico, é possível identificar funcionalidades que as aplicações de internet devem possuir para estar em conformidade com a legislação, não somente pelo que expressamente é exigido, mas pela característica de preservação dos direitos dos usuários pelo respeito ao desenvolvimento da personalidade e exercício da cidadania em meios digitais, fundamento amparado pelo Marco Civil da Internet (HAIKAL, 2017).

Pesquise mais

Entre essas "funcionalidades" estão as políticas de privacidade e os termos de uso das aplicações. Tais documentos devem prever o respeito ao direto de terceiros, bem como ferramentas que possibilitam eventuais abusos. Caso queira saber mais, sugerimos a leitura dos termos de uso do Facebook, a rede social mais acessada pelos brasileiros atualmente.

DECLARAÇÃO de direitos e responsabilidades. **Facebook**, 30 jan. 2015. Disponível em: <https://www.facebook.com/legal/terms>. Acesso em: 20 jun. 17.

Em relação à temática normativa, o principal ponto que vincula os direitos da personalidade e a internet, segundo a Lei do Marco Civil, concentra-se na proteção da privacidade e dos dados pessoais (art. 3º, II e III), garantindo-se a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação. Vejamos:

> **Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:**
> **[...]**
> **II - proteção da privacidade;**
> **III - proteção dos dados pessoais, na forma da lei. (BRASIL, 2014, art. 3º)**

Na contemporaneidade, em que o papel da internet se sobressai para as atuais gerações, onde todos os dados pessoais circulam e onde tudo acontece, os paradigmas da "sociedade da informação" se especificam com a "sociedade de serviços", o que traz como consequência dois fatos importantes: quanto mais o indivíduo deixa nas mãos do fornecedor do serviço uma cota relevante de informações pessoais; quanto mais a rede de serviços se alarga; mais crescem as possibilidades de interconexões entre bancos de dados e de disseminação internacional das informações coletadas (RODOTÀ, 2008, p. 100).

Nesse sentido, a Lei de Proteção de Dados, em seu Capítulo III, intitulado "Dos Direitos do Titular", especificamente em seu artigo 17 e seguintes dispõe que toda pessoa natural tem assegura a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, podendo obter do

controlador, mediante requisição e garantidas as exceções legais previstas, os dados por ele tratados. Assim, verificamos que a constante possibilidade de tensão entre direitos ou garantias fundamentais está diretamente associada à forma pela qual o titular possa interferir, pelo exercício de seus direitos, na esfera jurídica alheia (PODESTA, 2015). Vale dizer que a quantidade de dados disponíveis na internet automaticamente faz aumentar a possibilidade de incidentes nos quais verifica-se o embate entre direitos de natureza fundamental. Ora, o exercício do direto de liberdade de expressão, em certas ocasiões irá interferir na esfera de direitos de terceiros, especialmente seu direito à honra, imagem ou privacidade.

A partir do momento em que o espaço virtual incrementa a compreensão de democracia, a conjugação dos fundamentos legais expostos no Marco Civil da Internet e na Lei de Proteção de Dados, conforme estudamos na Seção 1.2, deveriam nortear toda a interpretação da lei. Todavia, ocorrem certas situações em que, inexoravelmente, os direitos lá dispostos entrarão em conflito. Tais conflitos serão normalmente resolvidos por meio do estabelecimento de salvaguardas ou prevalência de um bem jurídico em detrimento de outro. Assim, os direitos da personalidade possuem caráter relativo, ou seja, não são absolutos.

Aqui, vale fazer um paralelo entre os direitos da personalidade e os direitos fundamentais. Não existe na doutrina uma posição pacífica acerca da possibilidade de se considerar os direitos da personalidade como direitos fundamentais.

Alguns autores afirmam que os direitos da personalidade não podem ser considerados fundamentais porque estão positivados no plano infraconstitucional, e direitos fundamentais devem estar necessariamente previstos na Constituição. Além disso, rechaçam a possibilidade de o legislador ordinário estabelecer, alterar e revogar direitos fundamentais com a mesma facilidade com que edita leis comuns.

Apesar desses apontamentos, optamos pelo entendimento de que os direitos da personalidade são direitos fundamentais. Primeiramente, porque os direitos da personalidade foram alçados ao nível de "direitos fundamentais" pela Constituição de 1988 e posteriormente positivados no plano privado pelo Código Civil de 2002.

Igualmente, entende-se que os direitos da personalidade decorrem do princípio da "dignidade da pessoa humana", conforme já visto, que serve como norma de caráter geral para a tutela desses direitos. Se não bastasse, podemos dizer que ambos resultam da mesma proteção à subjetividade do ser humano.

Assim, é possível concluirmos que, apesar de haver uma diferenciação essencialmente doutrinária entre direitos fundamentais e direitos da personalidade, na maioria das vezes ambos irão resguardar o mesmo bem jurídico.

Por exemplo, a privacidade, a liberdade de expressão e a honra podem ser classificadas ora como direitos da personalidade, ora como direitos fundamentais. O essencial é sabermos que tais direitos possuem caráter relativo e que existem situações em que entram em conflito entre si. Assim, a mesma solução encontrada para os conflitos entre direitos fundamentais servirá para a resolução de conflitos entre direitos da personalidade.

Em se tratando de colisões entre os citados direitos, é necessário admitirmos o caráter "relativo" destes direitos. Para o professor Norberto Bobbio, o caráter absoluto dos direitos fundamentais (ou, em nosso caso, dos direitos da personalidade) não passa de uma mera "ilusão". Isso porque a história demonstra que os direitos fundamentais formam uma classe variável no tempo e no espaço (BOBBIO, 1992).

Nesse sentido, direitos que foram declarados absolutos e invioláveis no final do século XVIII, como a propriedade, foram submetidos a radicais limitações nas declarações contemporâneas; direitos que as declarações do século XVIII nem sequer mencionavam, como os direitos sociais, são agora proclamados com grande ostentação nos recentes documentos.

No futuro poderão emergir novas pretensões, inimagináveis no momento, como o direito de respeitar a vida dos animais. Assim, não existem direitos fundamentais "por natureza"; o que parece fundamental em uma época histórica e em uma determinada civilização não se afigura fundamental em outras épocas e outras culturas. O argumento de Bobbio é perfeitamente aplicável nos dias de hoje, eis que o desenvolvimento de novas tecnologias impõe novos desafios ao convívio social.

A respeito da colisão de princípios, nos ensina o jurista e filósofo Alexy que, quando dois princípios entram em colisão, um dos dois

princípios tem que ceder ante o outro. Mas isso não significa declarar inválido o princípio "desprezado". Na verdade, o que acontece é que, submetida a certas circunstâncias, pode ser que um dos princípios se sobreponha ao outro e vice-versa (ALEXY, 2002).

Contextualizando à nossa temática, podemos dizer que, em determinadas situações, a proteção à privacidade e aos dados pessoais poderá se sobrepor à liberdade de expressão e, em outras, a liberdade de expressão será mais importante que a privacidade. Tudo depende da avaliação do julgador no caso concreto.

Exemplificando

Um exemplo clássico do conflito entre liberdade de expressão e outros direitos da personalidade (ambos fundamentais) diz respeito à quebra do sigilo de dados pessoais em situações em que há um excesso de liberdade de expressão. Por exemplo, caso uma pessoa realize uma publicação com conteúdo ilícito, por meio de um perfil falso em uma rede social, tal pessoa poderá ter seus dados pessoais e registros de atividade revelados por meio de ação judicial intentada pela pessoa que foi ofendida na publicação on-line.

Alexy (2002) continua seu argumento, afirmando que havendo colisão entre direitos fundamentais, em sua avaliação, deve o julgador utilizar-se de um "critério de proporcionalidade", para que assim seja dado e reconhecido como prevalente o bem de maior peso ou envergadura jurídica, e que ainda não cause prejuízo à dignidade da pessoa, em nosso caso, o usuário da internet. Daí a importância do estudo da proporcionalidade, como sugestão de critério para fornecer meios ao julgador, a fim de que se encontre a melhor solução para resolver tais colisões.

O princípio da proporcionalidade, também chamado de proibição do excesso, teve como origem o princípio da razoabilidade nos Estados Unidos, e sua sede, em tese, no Direito Administrativo, por meio do controle do poder de polícia, de onde foi alçado à esfera constitucional. Possui aplicação inquestionável em muitos países, agindo como bússola norteadora em muitos julgados, pois tem a finalidade de estabelecer o equilíbrio entre conflitos de interesses, determinando qual deverá prevalecer ao caso concreto. No Brasil, apesar de inexistir dispositivo específico tratando da matéria, nossa

Constituição Federal o incorporou implicitamente, notadamente no que tange à proteção dos direitos e garantias dos cidadãos, e a jurisprudência, na maioria das vezes, encontra supedâneo legal no artigo 5º, LIV, da CF/88, no princípio do devido processo legal, visando suprir a lacuna legal (BARROS, 2003).

Podemos dizer que o princípio da proporcionalidade consiste na verificação pelo juiz, quando diante de dois interesses, se são juridicamente protegidos. Em caso afirmativo, deverão tais interesses ser ponderados e pesados dentro do critério da proporcionalidade, que estabelecerá os limites e a atuação das normas na verificação do interesse predominante. Os interesses postos em conflito são balanceados. Cabe ao julgador, através da análise desses interesses, decidir em que medida um prevalece sobre o outro (SZANIAWSKI, 1993).

Assim, pela perspectiva do princípio em fomento, os direitos e garantias constitucionais contemplados também no Marco Civil da Internet só poderão ser limitados em casos expressamente previstos pela Constituição e, excepcionalmente, quando necessário, para preservar outros direitos de igual hierarquia jurídica, sendo que a intenção foi justamente salvaguardar o núcleo essencial dos direitos e garantias previstos em Constituição.

Nesse diapasão, a importância do princípio da proporcionalidade, na hipótese de conflitos entre princípios constitucionais, reside na busca pelo ponto de equilíbrio entre os interesses em jogo, e que aparentemente se encontram em situação de conflito. Para o tema em análise, é ainda necessário verificar se as medidas judiciais adotadas na solução do problema concreto apresentam-se necessárias, razoáveis e sem excesso, de modo que não existam outros meios, menos invasivos, capazes de solucionar os problemas advindos daquele conflito.

Reflita

Seria a ponderação a melhor maneira de resolver eventuais conflitos entre direitos fundamentais ou entre direitos da personalidade? Quais as vantagens e desvantagens do uso da proporcionalidade como ferramenta de solução desses conflitos? Haveria um eventual "enfraquecimento" do direito mitigado em detrimento de um outro?

Portanto, temos que os direitos da personalidade, consagrados em nosso ordenamento jurídico, não foram esquecidos pelo legislador no tocante à regulação do espaço virtual. Pelo contrário, o Marco Civil da Internet colocou em destaque princípios como intimidade e proteção de dados pessoais, bem como a própria liberdade de expressão, que serão mais profundamente estudados na próxima sessão. Ademais, tais direitos, inexoravelmente, irão entrar em conflito, tendo em vista os diferentes interesses dos principais *players* ou atores da internet, nominalmente, os usuários, o Estado e os provedores de serviços.

Pesquise mais

Para saber mais sobre os "Direitos da Personalidade na Sociedade da Informação", sugerimos a leitura do artigo de mesmo nome, de autoria de Victor Auilo Haikal.

Disponível em: <http://digitalrights.cc/blog/2017/03/06/direitos-de-personalidade-na-sociedade-da-informacao/>. Acesso em: 13 maio 2017.

Pronto para elaborar a sua notificação extrajudicial?

Sem medo de errar

Estabelecidos os conceitos desta seção, vamos resolver nossa situação-problema? Relembrando que devemos redigir uma breve notificação extrajudicial, objetivando a remoção de um conteúdo ilícito publicado no blog de João Falastrão. Para resolvermos essa questão, iremos precisar retomar o conceito de direito da personalidade, seus mecanismos de proteção, tanto em âmbito constitucional como infraconstitucional. Ademais, devemos analisar a estrutura de uma notificação extrajudicial. Na mesma, deverão constar o destinatário da mensagem, a qualificação das partes, a breve síntese dos fatos, os direitos do Notificante que foram violados e as medidas a serem tomadas pelo Notificado, bem como as eventuais penalidades ou consequências em caso de inobservância dessas medidas. Vamos lá?

A
"João Falastrão"
[Endereço eletrônico a ser enviada a notificação]

Referência: Notificação extrajudicial para remoção de conteúdo ilícito de site da internet.

Prezado senhor "João Falastrão"

"POLÊMICO OLIVEIRA" [qualificação pessoal com endereço completo] vem por meio de seu procurador abaixo assinado, apresentar a presente **NOTIFICAÇÃO EXTRAJUDICIAL**, o que o faz nos seguintes termos:

Na data de DD/MM/AAAA, V. Sa., publicou, em seu blog pessoal, hospedado no endereço www.joaofalastrao.com.br, conteúdo ilícito que viola a honra e imagem do Notificante. O referido conteúdo relata a prática de atividades criminosas por parte do deputado Polêmico Oliveira. Tais acusações, destituídas de qualquer tipo de prova documental ou testemunhal, não passam de meras ilações que têm por objetivo único prejudicar a reputação do Notificante perante seus eleitores.

Trata-se de violação aos direitos da personalidade do Notificante, especificamente sua honra e imagem, os quais encontram guarida na Constituição Federal de 1988, especificamente em seu artigo 5º, inciso X.

Assim, deve V. Sa. remover o conteúdo apontado nesta notificação extrajudicial, no prazo de 24 (vinte e quatro) horas, contado do recebimento do presente documento, sob pena de responder judicialmente pelas perdas e danos provocados ao Notificante.

Local e data

Assinatura do representante do Notificante

Avançando na prática

Resolvendo conflitos entre direitos fundamentais e direitos da personalidade na internet

Descrição da situação-problema

Determinado aplicativo de mensagens instantâneas estava sendo usado por uma quadrilha de criminosos como ferramenta para troca de mensagens e informações. Diante do ocorrido, a Polícia Federal requereu a quebra de sigilo de dados dos investigados, de modo a obter acesso aos registros de atividades executadas por esses criminosos, bem como os dados pessoais deles, os quais encontram-se armazenados nos servidores do provedor de aplicação responsável por tal aplicativo. Na condição de magistrado que recebeu tal pedido da Polícia Federal, você emitiria um mandado determinando a revelação desses dados pessoais? Para resolver tal questão, você deverá levar em consideração os direitos em conflito e mostrar como resolvê-lo no caso concreto.

Resolução da situação-problema

Primeiramente, devemos identificar os direitos da personalidade ou direitos fundamentais que estão em aparente conflito na situação narrada. Por um lado, temos o direito à privacidade das pessoas investigadas e, consequentemente, o direito à proteção de seus dados pessoais na condição de usuários dos serviços de aplicação de internet narrados. Doutro lado, temos o direito à segurança pública, que se trata de um interesse coletivo e difuso, cuja tutela cabe ao Estado.

A respeito da colisão de princípios, nos ensina o jurista e filósofo Alexy que, quando dois princípios (ou direitos) entram em colisão, um dos dois princípios tem que ceder ante o outro. Mas isso não significa declarar inválido o princípio "desprezado". Na verdade, o que acontece é que, submetida a certas circunstâncias, pode ser que um dos princípios se sobreponha ao outro.

O jusfilósofo continua seu argumento, afirmando que havendo colisão entre direitos fundamentais, em sua avaliação, deve o julgador utilizar-se de um critério de proporcionalidade, para que assim seja dado e reconhecido como prevalente o bem de maior peso ou envergadura jurídica, e que ainda não cause prejuízo à dignidade da pessoa, em nosso caso, o usuário da internet.

Assim, na condição de juiz, você deverá verificar se ambos os direitos em aparente conflito são juridicamente protegidos. Nesse caso, tanto o direito à privacidade quanto a segurança pública encontram guarida em nosso ordenamento jurídico. Assim, tais interesses deverão ser ponderados e pesados dentro do critério da proporcionalidade, que estabelecerá os limites e a atuação das

normas na verificação do interesse predominante.

Dessa maneira, caso existam elementos convincentes de que os usuários daquela aplicação estejam cometendo algum tipo de ilícito, é cabível a quebra de sigilo de seus dados pessoais, tratando-se de verdadeira decisão proporcional, dados os interesses sociais em conflito.

Faça valer a pena

1. Dentro de uma sistemática organizacional, os direitos da personalidade distribuem-se em duas categorias gerais: "adquiridos" e "_____". Os primeiros existem nos termos e na extensão da disciplina do direito. Os segundos se sobrepõem a qualquer condição legislativa, sendo absolutos, irrenunciáveis, intransmissíveis e imprescritíveis.
Assinale a única alternativa correta que preenche a lacuna.
a) nativos.
b) naturais.
c) distintivos.
d) inatos.
e) congêneres.

2. Em linhas gerais, os direitos da personalidade envolvem o direito à vida, à liberdade, ao próprio corpo, à incolumidade física, à proteção da intimidade, à integridade moral, à preservação da própria imagem, nome, às obras de criação do indivíduo e tudo mais que seja digno de proteção, amparo e defesa na ordem jurídica.
Levando-se em consideração as diversas aplicações de internet existentes, que potencializaram todos os atos da vida particular e profissional de quem as utiliza, é natural que:
a) as projeções da personalidade fiquem restritas ao meio físico.
b) exista a ampliação da projeção da personalidade de quem executa determinadas ações nesses ambientes digitais.
c) não haja mudança de paradigma na manifestação dos direitos da personalidade.
d) não haja necessidade das aplicações estarem em conformidade com a legislação, sobretudo em relação à proteção individual dos usuários.
e) haja um alongamento das distâncias entre indivíduos, o que diminuiria eventuais violações e ofensas aos direitos da personalidade dos usuários de internet.

3. O princípio da proporcionalidade, também chamado de proibição do excesso, teve como origem o princípio da razoabilidade nos Estados Unidos, e sua sede, em tese, no Direito Administrativo, por meio do controle do poder de polícia, de onde foi para a esfera constitucional. Possui aplicação inquestionável em muitos países, agindo como bússola norteadora em muitos julgados, pois tem a finalidade de estabelecer o equilíbrio entre conflitos de interesses, determinando qual deverá prevalecer ao caso concreto.

No Brasil, apesar de inexistir dispositivo específico tratando da matéria, nossa Constituição Federal o incorporou implicitamente, notadamente no que tange à proteção dos direitos e garantias dos cidadãos, e a jurisprudência, na maioria das vezes, encontra supedâneo legal no artigo 5º, LIV, da CF/88, no seguinte princípio do(a):

a) lealdade.
b) isonomia.
c) ampla defesa.
d) legalidade.
e) devido processo legal.

Seção 2.2

Liberdade de expressão e privacidade na internet

Diálogo aberto

Então, caro aluno, depois que falamos na seção anterior sobre os direitos da personalidade, vamos apresentar a você, nesta oportunidade, alguns aspectos sobre liberdade de expressão e a privacidade na internet. É muito comum que no ambiente digital existam conflitos entre direitos de igual natureza, porém contrastantes entre si. De maneira recorrente vemos conflitos entre liberdade de expressão e direito à privacidade ou proteção de dados pessoais. Um exemplo de conflito foi retratado em nosso contexto de aprendizagem, no qual o blogueiro João Falastrão publicou um conteúdo, muito difundido nas redes sociais, acusando o deputado Polêmico Oliveira de corrupção passiva.

Para esta Seção 2.2, iremos trabalhar com a seguinte situação-problema: considerando que o conteúdo publicado no blog de João tenha sido reproduzido em diversos outros blogs, de modo que, ao utilizar uma ferramenta de busca on-line, tais notícias figurem na primeira página dos resultados, e considerando que o deputado foi inocentado das acusações de corrupção, é possível remover tais conteúdos da página de resultados dos diferentes motores de busca na internet no Brasil? Qual é o fundamento jurídico a ser utilizado em eventual peça de ingresso de um processo intentado pelo deputado Polêmico contra o blogueiro João?

Para resolver tal questão, iremos analisar o direito de privacidade aplicado à internet, bem como eventuais conflitos com o direito à liberdade de expressão, além das questões relacionadas ao direito ao esquecimento.

Lembre-se de que para esta unidade, além da notificação, trabalharemos com uma petição inicial, requerendo a remoção dos conteúdos do blog de João.

Não pode faltar

Conforme temos falado ao longo dos nossos estudos, a evolução dos meios tecnológicos e a influência deles sobre nosso modo de vida atual ocasionaram profundas mudanças sobre nosso sistema jurídico e seus institutos. A título de exemplo, podemos fazer as seguintes indagações: será que o conceito de direito de privacidade da década de 1980, idealizado pelo constituinte brasileiro, é idêntico ao conceito de privacidade que temos hoje? Será que a exposição voluntária à qual nos submetemos tem o condão de alterar esse conceito de privacidade? Qual é o papel das redes sociais no tema? É possível vivermos em um mundo "à parte" do digital?

Fato é que a tecnologia, especificamente aquela voltada para o tratamento automatizado de informações pessoais, tem um impacto tremendo sobre os direitos fundamentais dos cidadãos. Certamente, aquele que mais vem sofrendo ingerências tanto do Estado quanto dos entes privados é o direito à privacidade ou intimidade. Esse direito, que já foi considerado como o "direito de ser deixado em paz", ou o direito de esconder de terceiros certos aspectos da vida privada, hoje assume contornos diferentes.

Falamos, atualmente, em "proteção de dados pessoais". O acúmulo de informações pessoais tanto pelo Estado, que informatizou diversos serviços prestados aos cidadãos (ex.: declaração do imposto de renda pelo meio eletrônico; utilização de urnas eletrônicas com biometria para exercício do voto), quanto pelo setor privado ocasionou a utilização dessas informações em proveito próprio. Naturalmente, surgiu a necessidade de se criar medidas capazes de contrabalancear essa tendência, de maneira a evitar abusos e resguardar os direitos da personalidade dos cidadãos.

Dessa maneira, surgiram, em diversos países, iniciativas para o estabelecimento de normas específicas a respeito da utilização de informações pessoais, entendida aqui como um espectro da própria privacidade. A partir de 1970, essa tendência consolidou-se em diversos países que, em razão de seu protagonismo tecnológico, tiveram de tratar especificadamente da proteção de dados pessoais, como a França e a Alemanha. Tais normativas comungavam dos mesmos princípios e técnicas, que são comuns, até hoje, em grande parte das legislações a respeito do tema (DONEDA, 2015).

Eles serão tratados como verdadeiros "princípios gerais" de proteção de dados pessoais. Iremos classificá-los da seguinte maneira:

a) Princípio da Transparência (ou Publicidade): dispõe que a existência de um banco de dados pessoais deve ser de conhecimento geral da população, sendo que as modalidades de utilização das informações pessoais devem ser amplamente divulgadas.

b) Princípio da Qualidade: os dados armazenados devem ser um retrato fiel da realidade, o que compreende a necessidade de que sua coleta e tratamento sejam feitos com cautela e correção, realizando-se atualizações constantes de tais dados.

c) Princípio da Finalidade: qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados.

d) Princípio do Livre Acesso: o titular dos dados pessoais armazenados deve ter acesso ao banco de dados onde suas informações estão armazenadas, podendo obter réplicas desses registros, bem como controlar a exatidão deles.

e) Princípio da Segurança Física e Lógica: dispõe que os dados devem ser protegidos contra os riscos de extravio, destruição, modificação, transmissão ou acesso não autorizado.

f) Princípio da Proporcionalidade: os dados pessoais somente podem ser tratados se forem relevantes e pertinentes em relação à finalidade para a qual foram coletados, evitando sua utilização excessiva.

g) Princípio da Necessidade: de acordo com esse postulado, devem ser coletados e tratados somente os dados pessoais que são necessários para o atendimento de uma determinada finalidade, descartando-se os dados exorbitantes.

Em relação a estes dois últimos, temos que o princípio da necessidade estaria, de certa maneira, contido no princípio da proporcionalidade. Todavia, ele vem se apresentando, recentemente, em algumas legislações, de forma autônoma, seja pela necessidade de se ressaltar que a utilização dos dados pessoais deve corresponder a uma utilidade específica, seja pelo fato de que o princípio da necessidade esteja ligado diretamente à ideia de minimização do uso de dados pessoais (DONEDA, 2015).

Exemplificando

Um exemplo de legislação em que o princípio da necessidade se apresenta de forma autônoma é a inglesa. Em relação ao processamento de dados pessoais, tal normativa preconiza que o tratamento deve ser feito de maneira não excessiva (proporcional) e adequada (necessária para atingir determinado propósito).

Esses princípios, ainda que dispersados ou adaptados, formam a coluna central de diversas leis, tratados, convenções ou acordos acerca da proteção de dados pessoais, formando o centro das questões com as quais o ordenamento jurídico deve enfrentar ao buscar sua própria solução ao problema apresentado (DONEDA, 2015).

É de se notar que o Brasil ainda não possui uma lei geral de proteção de dados pessoais, o que indica certo atraso em relação a outros países, inclusive vizinhos, como Chile e Argentina. Nesse sentido, encontra-se em tramitação o Projeto de Lei nº 5.276, de 2016, que trata justamente sobre a temática.

Reflita

Em que pese a discussão sobre o tema e sua relevância, devemos parar e pensar por que o Brasil ainda não possui uma lei geral de proteção de dados pessoais. Qual seria essa razão? Seria porque o brasileiro não se preocupa com o destino de seus dados pessoais nem o que os provedores de serviços na internet ou o próprio Estado fazem com esses dados? Seria em razão de nossa herança militar e de ingerência do Estado sobre a vida dos cidadãos? Ou seria simplesmente porque o processo legislativo brasileiro é lento para dirimir questões voltadas para internet e novas tecnologias?

Apesar de não termos uma legislação geral, os citados princípios de proteção de dados pessoais encontram-se consubstanciados em regras específicas na legislação infraconstitucional. A título de exemplo, podemos citar o Código de Defesa do Consumidor, em seus artigos 43 e 44, os quais tratam sobre a formação e manutenção de bancos de dados contendo cadastro de consumidores. Ademais, podemos citar a Lei do Cadastro Positivo (Lei nº 12.414, de 2011), a Lei de Acesso à Informação (Lei nº 12.527, de 2011, a Lei de Proteção de Dados (Lei nº 12.965, de 2014) e o próprio Marco Civil da Internet.

Todas elas trazem, de forma clara, alguns dos princípios de proteção de dados pessoais já elencados.

Todavia, o direito de privacidade e, consequentemente, a proteção de dados pessoais não podem ser considerados como algo absoluto ou ilimitado. Conforme vimos na Seção 2.1, não existem direitos absolutos, mesmo os direitos fundamentais, ou intrínsecos à personalidade, podem sofrer, em determinadas condições, certas limitações, sobretudo se confrontados com outros direitos de igual natureza e envergadura jurídica.

Se não bastasse, o direito de privacidade jamais é oponível perante ordem judicial específica. Um magistrado pode, de ofício, ou face ao pedido de uma autoridade administrativa, requisitar informações e dados pessoais de determinada pessoa, face à conveniência de determinada investigação ou no curso de processo, cível ou criminal.

A inviolabilidade da vida privada resta igualmente comprometida face à segurança pública ou repressão penal. Aliás, vivemos em um mundo cada vez mais conectado e, igualmente, vigiado. Constantemente nos deparamos com escândalos envolvendo a privacidade de pessoas e autoridades.

Exemplificando

A título de exemplo, podemos citar o caso Snowden, que revelou a espionagem digital sobre mensagens privadas de líderes mundiais, como a ex-presidente Dilma Rousseff e a primeira-ministra alemã, Angela Merkel. Para saber mais sobre o caso, sugerimos a leitura da reportagem disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 1 maio 2017.

Particularmente delicada é a questão dos limites do direito à privacidade face à liberdade de expressão, que por sua vez abarca a exteriorização de pensamentos, ideias, opiniões, convicções, bem como sentimentos em suas mais variadas formas, como atividades intelectuais, artísticas, científicas e de comunicação. Nesse sentido, nos termos da Constituição Federal de 1988, dispõe que: "é livre a manifestação do pensamento, sendo vedado o anonimato" (BRASIL, 1988, art. 5º, inc. IV), trata-se de direito fundamental e de idêntica envergadura jurídica ao direito de privacidade.

O exercício da liberdade de expressão é o exercício de uma liberdade civil e política. Sem comunicação livre não se pode falar em sociedade livre e muito menos em Estado democrático. A liberdade de expressão exerce uma função tríplice: formação de opinião pública; instrumento para o exercício de demais direitos; e controle dos poderes públicos.

É comum que o referido direito entre em conflito com outros de igual natureza jurídica. De maneira mais recorrente, podemos citar o direito à imagem, à honra e à privacidade. Reparem que o direito de liberdade de expressão, ao mesmo tempo que atua como limitador à privacidade, é limitado por tal direito. Como vimos anteriormente, cabe ao julgador, levando em consideração as particularidades do caso concreto, bem como a proporcionalidade e razoabilidade, decidir qual desses direitos irá prevalecer sobre o outro naquele caso específico.

Tal conflito entre direitos é ainda agravado em um mundo onde as pessoas estão cada vez mais interligadas pela internet. O fluxo de informações nunca foi tão grande e dinâmico, sendo que violações tanto à privacidade quanto à liberdade de expressão tornaram-se comuns. O embate entre os citados direitos fundamentais encontrou, recentemente, uma nova faceta. Trata-se do chamado "direito ao esquecimento" (do original, *right to be forgotten*).

Assimile

Direito ao esquecimento é a faculdade de obstar o processamento informatizado, a transferência ou publicação de dados pessoais, além de exigir que sejam apagados, sempre que sua preservação esteja causando constrangimento ao sujeito envolvido, desde que não haja razão de interesse público que justifique a preservação (PARENTONI, 2015).

De um lado, há quem sustente que cabe ao indivíduo se deseja ou não tornar públicos certos aspectos de sua vida privada. Nesse sentido, o direito da privacidade abarcaria a prerrogativa do sujeito de retirar da internet informações a seu respeito. Em sentido oposto, há quem faça uma ponderação entre a pretensão individual ao esquecimento e o interesse coletivo de certas informações, de maneira a justificar a publicação e a preservação destas últimas, mesmo contra a vontade dos envolvidos.

O Superior Tribunal de Justiça, corte de nosso país, julgou dois *leading cases* acerca do direito ao esquecimento. No REsp nº 1.334.097-RJ, houve o reconhecimento do direito ao esquecimento em ação intentada contra uma famosa emissora de televisão, por pessoa apontada como coautora da Chacina da Candelária, mas que fora absolvida em júri popular. O autor pleiteou danos morais por ter seu nome exposto em programa policial, trazendo-lhe a pecha de assassino e violando sua privacidade.

A ação foi definida como procedente, sendo a emissora condenada a uma vultosa indenização. O relator, ministro Luiz Felipe Salomão, em seu acórdão, fez uma dicotomia relevante entre o direito à liberdade de expressão e o direito ao esquecimento, entendido aqui como um aspecto do direito à privacidade, tendo como norteador o princípio da dignidade da pessoa humana. Conclui-se que, não havendo interesse público na exposição e já tendo ocorrido a absolvição do acusado, a ponderação de princípios levaria à preferência, neste caso, pela proteção da intimidade e da privacidade do autor.

Por outro lado, no julgamento do Recurso Especial nº 1.335.153-RJ, o mesmo ministro-relator entendeu haver interesse público na exibição, por se tratar de um fato histórico, tendo entrado para domínio público. O relator fundamentou sua decisão na impossibilidade de exercício da atividade de imprensa sem citar o nome da vítima, visto que já haviam passado 50 anos do crime.

Atualmente, o tema encontra-se sob apreciação do Supremo Tribunal Federal, que decidirá acerca da existência, ou não, de um direito ao esquecimento no ordenamento jurídico brasileiro, bem como seus eventuais limites e quais os critérios a serem observados pelo julgador diante do caso concreto.

O assunto ilustra bem a proteção ampla conferida pela Constituição Federal tanto à liberdade de expressão quanto à privacidade. Tais direitos constantemente entram em conflito, sendo que a internet se apresenta como novo palco para esse confronto. Nesse sentido, não podemos deixar de citar o caso envolvendo a subsidiária do Google na Espanha.

O referido caso foi julgado em 2014 pelo Tribunal de Justiça da União Europeia, que, por sua vez, consolidou o entendimento de que os motores de busca na internet, aqueles que percorrem a rede em busca de informações, realizam tratamento de dados pessoais, nos termos da Diretiva nº 1995/46/CE, ainda que se limitem a indicar onde

se encontra a informação, sem qualquer interferência ou controle sobre a fonte de dados. Destarte, podem ser compelidos a remover resultados de busca, ainda que os dados permaneçam disponíveis na fonte original, desde que não haja interesse público na divulgação daquele fato.

Pesquise mais

Para saber mais sobre o caso *Google v. Mario Gonzáles*, sugerimos a leitura de artigo de autoria do professor Otávio Rodrigues sobre a decisão, disponível em: <http://www.conjur.com.br/2014-mai-21/direito-apagar-dados-decisao-tribunal-europeu-google-espanha>. Acesso em: 7 jun. 2017.

Portanto, concluímos que o direito ao esquecimento apresenta fundamento jurídico e deve ser admitido no ordenamento jurídico brasileiro, respeitando-se certos pressupostos e limites. Além disso, sua forma mais eficaz (e provavelmente mais polêmica) é quando atinge os motores de busca da internet, ao invés da fonte original dos dados ou informação.

Sem medo de errar

Vistos os conceitos da unidade, vamos resolver nossa situação-problema? Lembremos de que neste ponto você irá apresentar solução à segunda parte do seu produto e, para tanto, iremos precisar elaborar uma breve petição inicial com pedido de remoção das publicações ofensivas feitas pelo blogueiro João ao seu cliente, o deputado Polêmico.

Vimos que o monitoramento prévio por parte dos sites de busca apresenta-se inviável e um risco, sobretudo, ao direito de liberdade de expressão. Além disso, mesmo se recorrermos à teoria do direito ao esquecimento, esbarraríamos na questão do cargo público ocupado pelo nosso deputado.

Ademais, ao longo desta resolução, iremos relembrar, superficialmente, também a estrutura de uma petição inicial.

Exmo. Sr. Juiz de Direito da ___ Vara Cível da Comarca de _____/__

POLÊMICO DE OLIVEIRA, (qualificação completa com endereço), vem perante V. Exa., por seu advogado abaixo assinado, com endereço profissional (incluir endereço), interpor a presente AÇÃO ORDINÁRIA, em face de **JOÃO FALASTRÃO** (qualificação completa com endereço), pelas razões de fato e de direito a seguir expostas:

DOS FATOS

(Fazer um breve relato dos fatos.)

DO DIREITO

A Constituição Federal de 1988, em seu artigo 5º, inciso X, resguarda a proteção à honra e intimidade dos cidadãos. Igualmente, resguarda a liberdade de expressão (art. 5º, inciso IV). No caso em tela, as publicações realizadas pelo requerido ofenderam a honra do autor, bem como violaram sua intimidade e a de sua família.

Em face de eventual conflito entre os direitos fundamentais do autor à honra e intimidade e o direito fundamental do réu de expressar livremente sua opinião, é recomendável que o julgador utilize um critério de proporcionalidade para resolução do caso concreto.

Uma vez que o autor foi inocentado de todas as falsas acusações de corrupção constantes no weblog do requerido, devem tais conteúdos ser imediatamente removidos, e, ainda, ser o réu condenado ao pagamento de indenização pelos danos morais causados, nos termos do artigo 186 c/c 927 do Código de Processo Civil.

DO PEDIDO

(Aqui deverá constar o pedido de remoção de conteúdos e indenização por danos morais, além de outros correlatos.)

DAS PROVAS

(Constar as provas que se pretende produzir durante o curso do processo.)

(local, data e assinatura do procurador)

Avançando na prática

Direito ao esquecimento no Brasil

Descrição da situação-problema

Determinada Associação de Veículos de Informação de Rádio e Televisão entrou em contato com você a fim de pedir uma opinião legal sobre um caso específico. Uma das associadas, uma emissora de televisão local, pretende criar um programa no qual são reencenadas cenas de crimes ocorridos no passado que causaram grande repercussão na comunidade local. Para tanto, a Associação gostaria de saber se a emissora de TV corre algum risco de pagar indenização aos criminosos ou suas famílias, em razão de eventual violação ao seu "direito ao esquecimento".

Resolução da situação-problema

O direito ao esquecimento pode ser entendido como a faculdade de obstar o processamento informatizado, a transferência ou publicação de dados pessoais, além de exigir que sejam apagados, sempre que sua preservação esteja causando constrangimento ao sujeito envolvido, desde que não haja razão de interesse público que justifique a preservação.

No Brasil, o Superior Tribunal de Justiça julgou dois *leading* cases acerca do direito ao esquecimento, como o REsp nº 1.334.097-RJ, no qual houve o reconhecimento do direito ao esquecimento.

Por outro lado, em outros julgamentos, como do Recurso Especial nº 1.335.153-RJ, o direito não foi reconhecido, em razão da existência de interesse público na exibição, por se tratar de um fato histórico, tendo entrado para domínio público. O relator fundamentou sua decisão na impossibilidade de exercício da atividade de imprensa sem citar o nome da vítima, visto que já havia passado 50 anos do crime.

Tendo em vista os citados julgados, é possível admitir que a emissora de TV e outras associadas à consulente correm o risco de arcar com pedidos de indenização pelos criminosos e seus familiares, salvo se os casos versarem sobre fatos dotados de relevância pública.

Faça valer a pena

1. A necessidade evitar abusos e resguardar os direitos da personalidade dos cidadãos deu ensejo a um movimento global, no sentido de se criar normas visando à proteção de dados pessoais frente às novas tecnologias. Os países mais avançados tecnologicamente começaram a discutir e criar tais normas, que guardavam entre si ideias ou princípios semelhantes.
O princípio que dispõe que os dados pessoais devem ser protegidos contra os riscos de extravio, destruição, modificação, transmissão ou acesso não autorizado é chamado de Princípio da:
a) Finalidade.
b) Qualidade.
c) Segurança.
d) Necessidade.
e) Proporcionalidade.

2. O princípio da _____ estaria, de certa maneira, contido no princípio da _____. Todavia, ele vem se apresentando, recentemente, em algumas legislações, de forma autônoma seja pela necessidade de se ressaltar que a utilização dos dados pessoais deve corresponder a uma utilidade específica, seja pelo fato de que o princípio da _____ esteja ligado diretamente à ideia de minimização do uso de dados pessoais.
Assinale a alternativa que contém as palavras adequadas às lacunas.
a) necessidade – proporcionalidade – necessidade.
b) proporcionalidade – necessidade – proporcionalidade.
c) necessidade – proporcionalidade – segurança.
d) proporcionalidade – finalidade – necessidade.
e) finalidade – proporcionalidade – finalidade.

3. O exercício da liberdade de expressão é o exercício de uma liberdade civil e política. Sem comunicação livre não se pode falar em sociedade livre e muito menos em Estado democrático. Nesse sentido, a liberdade de expressão exerce uma função tríplice.
Assinale a alternativa que apresenta uma dessas funções:
a) Garantia de obrigações contratuais.
b) Controle dos poderes públicos.
c) Proteção da privacidade.
d) Garantia do anonimato.
e) Possibilidade de censura prévia.

Seção 2.3

A responsabilidade civil no Marco Civil da Internet

Diálogo aberto

Olá, aluno! Nas seções anteriores, estudamos o conceito de direito da personalidade e os mecanismos de resolução de conflitos entre tais direitos. Destacamos a questão do embate entre a privacidade e a liberdade de expressão, muito presente no cotidiano da internet. Agora iremos analisar o papel dos provedores nesse imbróglio, notadamente sua responsabilidade civil por conteúdos publicados por seus usuários e o dever de guardar registros eletrônicos.

Vamos relembrar o nosso contexto de aprendizagem? Então, temos que nosso cliente, o deputado Polêmico Oliveira, está sendo duramente atacado pelo blogueiro João Falastrão, que por sua vez publicou diversos conteúdos que afrontam a honra e a imagem do nosso cliente. Tais conteúdos foram inclusive replicados nas redes sociais de Falastrão, alcançando um número ainda maior de pessoas. Nesse sentido, iremos considerar a seguinte situação-problema:

Caso João tenha replicado o conteúdo ofensivo em seus perfis pessoais nos sites de redes sociais (ex.: Facebook, Twitter), seria possível pedir algum tipo de indenização contra esses provedores? Ainda, como se dá a responsabilidade civil dessas empresas perante conteúdos gerados por terceiro? Ao responder esses questionamentos, você deverá incluir um tópico em sua petição inicial discorrendo acerca da obrigação de remoção do conteúdo por parte dos provedores de aplicação e sua consequente responsabilidade civil. Assim vamos finalizar o nosso produto, a notificação extrajudicial e a petição inicial para fornecimento de dados e remoção de conteúdo de blog.

Ao longo desta seção iremos mobilizar diversos conhecimentos com o objetivo de resolver a situação-problema proposta. Iremos traçar uma linha evolutiva da jurisprudência tratando sobre a responsabilidade civil dos provedores de internet sobre os atos praticados por seus usuários. Iremos analisar os diferentes tipos de provedores de internet, bem como sua classificação no Marco Civil da Internet (MCI) e na doutrina.

Não pode faltar

A responsabilidade civil por veiculação na internet de conteúdo gerado por terceiro era tema que despertava intensos debates nos tribunais brasileiros mesmo antes da promulgação do Marco Civil da Internet. Enquanto vítimas de conteúdos inverídicos ou difamatórios buscavam reparação, empresas titulares de aplicativos de redes sociais e sites de relacionamento sustentavam que não podiam ser responsabilizadas por conteúdos inseridos por outros usuários, vez que não seria possível monitorar todo o material publicado em seus sites.

Embora o quadro jurisprudencial fosse bem diversificado, analisando a evolução das decisões proferidas, percebia-se um avanço rumo à superação da tese da irresponsabilidade das citadas empresas. Estas, por sua vez, vinham sendo condenadas pelos diferentes tribunais brasileiros pelos danos decorrentes de conteúdos publicados por seus usuários. Tais decisões fundavam-se em duas normas.

Primeiramente, no artigo 14 do Código de Defesa do Consumidor, reconhecendo-se também a existência de relação de consumo entre as empresas titulares dos sites e seus usuários, embora o serviço fosse prestado de maneira gratuito. Vejamos o que diz a referida norma:

> 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. (BRASIL, 1990, art. 14)

Em segundo lugar, apelava-se à norma contida no artigo 927, parágrafo único, do Código Civil Brasileiro, inserindo as atividades de exploração de sites de redes sociais e relacionamento no rol de atividades de risco, tendo em vista o elevado potencial de danos inerentes à criação de um espaço onde o conteúdo inserido assume dimensão pública, sem nenhum tipo de filtragem prévia. Vejamos:

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. (BRASIL, 2002, art. 927)

Assimile

Ambos os artigos se pautam na teoria da "responsabilidade objetiva". Recorda que a responsabilidade civil se pauta em quatro elementos? São estes: a) conduta comissiva ou omissiva; b) culpa (em sentido amplo); c) nexo de causalidade; d) dano sofrido pela vítima. Na teoria da reponsabilidade objetiva, desconsidera-se o elemento "culpa", tendo em vista a natureza da relação havida entre as partes ou a natureza da própria atividade (ato) praticada.

Sem desconsiderar a dificuldade técnica de monitoramento prévio do conteúdo publicado, os tribunais brasileiros vinham apontando medidas que poderiam ser adotadas pelas empresas titulares das redes sociais para prevenir ou atenuar os danos causados, como a identificação inequívoca do indivíduo que divulga o conteúdo falso ou difamatório, bem como mecanismos de denúncia por outros usuários.

Referidas decisões que levavam em consideração as citadas dificuldades técnicas não concluíam, em sua maioria, pela irresponsabilidade das empresas, mas sim por uma espécie de "responsabilidade condicionada", deflagrada tão somente a partir do momento em que, comunicada da existência do material lesivo, deixava de adotar providências para retirar o referido material do site.

Entretanto, saliente-se que tal comunicação poderia ser efetivada pela via extrajudicial, notadamente por meio de notificação, conforme tratamos na Seção 2.1. Assim, consolidou-se o entendimento, no âmbito dos tribunais regionais, de que os provedores responderiam por conteúdos ofensivos tão logo notificados, caso não os retirassem de seus sites. A fim de ilustrar tal situação, podemos citar aqui acórdão proferido pela 4ª Câmara Cível do Tribunal de Justiça do Rio de Janeiro em caso versando sobre a extinta rede social Orkut (TJRJ – AP 2008.001.04540, Rel. Des. Horácio Neto, j. 25/03/2008).

Pesquise mais

O envio de notificação extrajudicial com objetivo de remoção de conteúdos on-line foi, em parte, inspirado no sistema de *notice-and-takedown*, previsto na lei estadunidense, especificamente no *Digital Millenium Act*. Para saber mais sobre esse sistema, recomendamos a leitura do artigo disponível em: <https://victorhugotmenezes.jusbrasil.com.br/artigos/441755140/mecanismos-europeus-de-controle-de-dados-na-internet>. Acesso em: 14 jun. 2017.

De maneira semelhante, os tribunais também enfrentaram o problema da preservação dos dados de origem dos conteúdos ofensivos produzidos. Embora não houvesse nenhuma norma específica, entendia-se que os provedores deveriam manter em suas bases de dados aqueles úteis à vítima, de modo a resguardar seus direitos, pelo prazo mínimo da ação de reparação civil de ilícitos extracontratuais, qual seja, três anos (artigo 206, § 3º, inc. V do Código Civil). Todavia, o assunto era polêmico, não havendo uma uniformidade na jurisprudência.

Uma vez editada a Lei nº 12.965, de 2014, tais matérias receberam tratamento positivado, o qual passaremos a analisar de maneira detalhada. Vamos lá?

Em primeiro lugar, o Marco Civil da Internet (MCI) distinguiu as espécies de provedores, conforme a natureza dos serviços prestados. Tal diferenciação pode ser verificada no artigo 5º, que a fez da seguinte maneira:

> Art. 5º Para os efeitos desta Lei, considera-se:
> [...]
> V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
> VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
> VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP. (BRASIL, 2014, art. 5º)

De maneira simplificada, podemos dizer que os provedores (serviços de administração de sistema autônomo) podem ser classificados em "provedores de conexão" e "provedores de aplicação".

Tal distinção revela porque, nos termos da lei, são igualmente distintas as responsabilidades de cada um dos diferentes tipos de provedores, conforme o tipo de serviço que prestam. Por isso, o artigo 13 do MCI previu a responsabilidade do administrador de

sistema autônomo de manter registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano, ressalvada a dilação a requerimento cautelar de autoridade policial ou do Ministério Público. Vamos conferir?

> **Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. (BRASIL, 2014, art. 13)**

Ainda em relação à provisão de conexão, o artigo 14 vedou a guarda dos registros de acesso a aplicações da internet: "Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet" (BRASIL, 2014, art. 14).

Já para o provedor de aplicação de internet, segundo o artigo 15, constituído na forma de pessoa jurídica que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos, impôs-se a obrigação de manter os registros de acesso à aplicação da internet, também em sigilo e ambiente controlado, pelo período mínimo de 6 (seis) meses, igualmente postergável a pedido de autoridade policial ou do Ministério Público:

> **Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. (BRASIL, 2014, art. 15)**

Está tudo OK? Então, agora que vimos a responsabilização civil dos provedores de acesso, vamos falar um pouco sobre o dever de guarda de registros de conexões e aplicações no Marco Civil da Internet. Os registros de conexão e acesso a aplicação somente podem ser disponibilizados mediante ordem judicial específica, restando vedados os pedidos genéricos e coletivos, inclusive pelas autoridades administrativas, o que visa impossibilitar práticas de monitoramento em massa.

Reflita

O monitoramento em massa é prática comum em diversos países, principalmente aqueles que mais sofrem com ataques terroristas, tais como Estados Unidos e Inglaterra. A cada dia descobrimos novos escândalos relacionados à espionagem digital. Inclusive, foi um desses escândalos, o caso Snowden, que impulsionou a aprovação do Marco Civil da Internet no Brasil. Todavia, aqui vale uma breve reflexão: será que a insegurança provocada por ameaças terroristas justifica o monitoramento dos cidadãos, a ponto de sua privacidade ser sacrificada? Será que existe alguma solução capaz de garantir a segurança sem violar a intimidade de terceiros?

Particularmente em relação à responsabilidade por danos decorrentes de conteúdo gerado por terceiro, os provedores de conexão ficaram isentos de qualquer responsabilidade, nos termos do artigo 18 do MCI, que dispõe que "o provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros" (BRASIL, 2014, art. 18).

No tocante aos provedores de aplicação, diferenciam-se as situações de conteúdos ofensivos, de um lado, e conteúdo de nudez ou atos sexuais de caráter privado, de outro. No primeiro caso, o artigo 19 estatuiu que o provedor somente será responsabilizado civilmente se, após, ordem judicial específica, não tomar providências para, no âmbito e limites técnicos de seus serviços, e dentro do prazo judicial assinalado, tornar indisponível o conteúdo. Vejamos:

> **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. (BRASIL, 2014, art. 19)**

Ainda, a ordem judicial específica deverá conter identificação clara e inequívoca do conteúdo, de modo a permitir sua localização. Tal identificação é, normalmente, feita por meio da indicação do URL (endereço eletrônico) onde o conteúdo encontra-se disponível.

Já no segundo caso, dispensou-se a ordem judicial, contentando-se o Marco Civil com a notificação extrajudicial do provedor, responsabilizando-o subsidiariamente se, depois de notificado, deixar de promover a indisponibilização do conteúdo indicado, nos termos do artigo 21 do citado diploma legal:

> **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. (BRASIL, 2014, art. 21)**

Em análise à disciplina do tema, o professor Marcel Leonardi aponta ser critério básico de definição da responsabilidade do provedor, pelo conteúdo ilícito gerado por terceiro, o controle que ele tenha sobre esse material (LEONARDI, 2005).

Daí ressalvar a distintiva atividade prestada pelos "provedores de *backbone*", os quais, conforme acentua, não possuem responsabilidade pelos ilícitos praticados pelos usuários, tal como os provedores de acesso, igualmente isentos de responsabilidade. Para os provedores de "correio eletrônico", "hospedagem" e "conteúdo", salienta o autor ser aplicável a regra geral estatuída no artigo 19 do MCI.

Cumpre esclarecer que a classificação doutrinária feita pelo professor Leonardi referente aos diferentes tipos de provedores de serviços de internet não foi adotada no Marco Civil da Internet, em que pese ser possível sua adequação.

Nesse sentido, classificam-se como "provedores de conexão", nos termos do MCI, os provedores de *backbone* (aquele que detém as estruturas de rede, capaz de possibilitar o tráfego de informações) e de "acesso" (fornecedor de serviços que possibilita o acesso de seus usuários à internet).

Pesquise mais

Já que estamos falando de backbone e estruturas de transmissão, você sabe como é a qualidade do tráfego da informação da Internet no Brasil? Veja o vídeo Olhar Digital - Satélite brasileiro transmite a 80 Gbps e vai levar internet para todo o país, disponível em: <https://www.youtube.com/watch?v=fZpioYQLh3c>. Acesso em: 18 jul. 2017.

Já nos "provedores de aplicações" estariam contidos os provedores de "correio eletrônico" (disponibiliza e presta serviços de armazenamento e troca de mensagens eletrônicas ou e-mails), "hospedagem" (que permite o armazenamento de sites, blogs, redes sociais, etc., com seus textos, imagens, sons e informações em geral) e "conteúdo" (disponibiliza e armazena, em seus servidores, informações criadas por terceiros ou por meios próprios).

Por fim, a responsabilidade dos provedores face à publicação de conteúdos que violem direitos autorais não foi tratada no Marco Civil da Internet, que delegou tal tarefa à "lei específica", nos termos do § 2º do artigo 19. Todavia, tal "lei específica", até o momento, não foi promulgada.

Exemplificando

Nos casos em que há a publicação de conteúdos ilícitos na internet, como aqueles que violam a honra, reputação e imagem, os provedores de conexão não respondem pelos danos causados pelo usuário autor daquela publicação. Por sua vez, os provedores de aplicação podem ser responsabilizados desde que, recebida ordem judicial específica, deixem de remover o conteúdo considerado ilícito. Isso não quer dizer que o envio de notificação extrajudicial se tornou medida inócua. Há casos em que os provedores de aplicação promovem a remoção de conteúdos após recebimento de notificação, por exemplo, casos em que determinada publicação viola os termos de uso daquele site onde foi publicada.

Outro aspecto polêmico diz respeito à responsabilidade civil dos motores de busca por conteúdos ilícitos indexados em sua página de resultados. Ora, o natural seria a vítima ajuizar ação judicial contra o titular do site ou usuário diretamente responsável pela publicação do conteúdo. Ocorre que, como vimos na seção anterior, existe um crescente movimento na direção do direito ao esquecimento, em que os próprios motores de busca têm a obrigação de remover o conteúdo ilícito replicado em sua plataforma.

É, meu caro aluno, como dissemos, o assunto é polêmico e encontra-se sob análise do Supremo Tribunal Federal, especificamente no julgamento do Recurso Extraordinário (RE) nº 1.010.606, no qual familiares da vítima de um crime rumoroso praticado nos anos de 1950 questionam sua utilização em programa televisivo e pedem indenização.

Todavia, acreditamos que o artigo 19 do Marco Civil da Internet tem o potencial de colocar um fim à discussão sobre a existência do direito ao esquecimento. Isso porque motores de busca são enquadrados no conceito legal de "provedor de aplicação", assim, somente seria responsabilizado no caso de descumprimento de ordem judicial específica ou face à inatividade após recebimento de notificação nos casos de nudez e cenas de sexo. Assim, somente mediante ordem judicial específica determinando o motor de busca a remover os conteúdos é que haverá responsabilização.

Caso um usuário encontre um conteúdo ofensivo hospedado na primeira página da busca do Google, este deverá acionar o site responsável por hospedar o conteúdo ofensivo, e não o próprio motor de busca, caso queira tornar indisponível tal conteúdo.

O site de buscas não possui responsabilidade por conteúdos publicados por terceiros hospedados em outros sites da internet. Por consequência, não há o dever de monitorar conteúdos que aparecem na página de resultados de pesquisa, sob pena de tal conduta configurar-se censura prévia, limitando assim o direito de liberdade de expressão.

Exemplificando

Na jurisprudência, temos alguns casos emblemáticos, como o da apresentadora Xuxa, no qual o Superior Tribunal de Justiça decidiu que a empresa Google não era responsável pelos conteúdos e imagens relativas à busca qualquer expressão cujo resultado associasse o nome artístico da apresentadora a alguma prática criminosa (REsp nº 1.316.921-RJ).

Concluindo, temos que o Marco Civil da Internet veio como ferramenta para acabar com as discussões acerca da responsabilidade civil dos provedores de internet. Se antes da aprovação da citada lei víamos decisões judiciais que atribuíam a responsabilidade civil objetiva, hoje em dia elas são praticamente inexistentes. O artigo 19

positivou, em certa medida, a "responsabilidade condicionada" dos provedores, porém sua notificação deve ser feita de maneira judicial, e não extrajudicial, salvo para os casos de cenas de nudez e atos sexuais de caráter privado, nos termos do artigo 21 do MCI.

Sem medo de errar

Vistos os conceitos relacionados à responsabilidade civil dos provedores de internet pelos atos praticados por seus usuários, já temos plenas condições de resolver nossa situação-problema, que, relembrando, trata-se da inserção de um tópico em nossa petição inicial tratando sobre a responsabilidade civil dos provedores de aplicação nos quais João Falastrão replicou o conteúdo ilícito e ofensivo ao nosso cliente, deputado Polêmico Oliveira. Vamos finalizar nosso produto?

PETIÇÃO INICIAL PARA FORNECIMENTO DE DADOS
E REMOÇÃO DE CONTEÚDO DE BLOG (cont.)

DO DIREITO

DA RESPONSABILIDADE DOS PROVEDORES
PELOS ATOS PRATICADOS POR TERCEIROS

Conforme visto anteriormente, o réu realizou publicações em seu blog pessoal com o objetivo único de ofender o autor, que teve seus direitos constitucionais à honra e imagem violados. Não bastasse a execração realizada em blog de sua titularidade, o réu replicou referidos conteúdos em seus perfis pessoais junto às redes sociais, especificamente o Facebook e Twitter. Se não bastasse, foi o réu notificado extrajudicialmente acerca da referida violação dos direitos do autor.

Diante do ocorrido, o autor, desde já, requer que sejam ambos os provedores incluídos no polo passivo da demanda e notificados para, no prazo a ser estabelecido por V. Exa., que removam os conteúdos publicados em seus sites, veiculados nos seguintes endereços eletrônicos (URLs):

(Listar as URLs onde os conteúdos ofensivos encontram-se hospedados)

Caso os provedores se recusem a remover o conteúdo, deverão responder civilmente pelos danos causados ao autor, nos termos do artigo 19 do Marco Civil da Internet:

> 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. (BRASIL, 2014, art. 19)

Nesse sentido, já se manifestou o egrégio Tribunal de Justiça de São Paulo:

> Ementa: INDENIZAÇÃO - DANOS MORAIS - CONTÉUDO CONSIDERADO OFENSIVO VEICULADO NA INTERNET AÇÃO PROPOSTA CONTRA O PROVEDOR DE HOSPEDAGEM - AUSÊNCIA DE RESPONSABILIDADE DO PROVEDOR, QUE NÃO TEM O DEVER DE FISCALIZAR O CONTEÚDO DAS MENSAGENS DE AUTORIA DE SEUS USUÁRIOS - AÇÃO IMPROCEDENTE - SENTENÇA MANTIDA - RECURSO NÃO PROVIDO. (Apl. 01655408220098260100 – 5ª Cam. Dir. Priv. – Rel. Des. Erickson Marques – DJ: 25/03/2015)

Ademais, deverão os provedores apresentar perante este juízo todos os dados cadastrais que possibilitem a identificação inequívoca do responsável pelas publicações realizadas, notadamente dados de *login*, número de IP e e-mail utilizado para realização do cadastro na respectiva rede social.

O dever de guarda de dados de aplicação decorre da norma contida no artigo 15 do Marco Civil da Internet:

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. (BRASIL, 2014, art. 15)

Finalizado o tópico relacionado aos fundamentos jurídicos da petição inicial, passamos para a parte do pedido, tratado na seção anterior.

Avançando na prática

Como resolver o problema do "caiu na net"

Descrição da situação-problema

Idalina, psicóloga de uma empresa comercial de grande porte, teve seu nome inserido, contra sua vontade, em um site de encontros românticos. Ao lado do seu nome completo e do seu verdadeiro número de telefone de trabalho, o site veiculava a seguinte informação: "pessoa que se propõe a participar de programas de caráter afetivo e sexual". Embaixo de tais dizeres, foram publicadas fotos íntimas de Idalina. Com receio de perder seu emprego por conta da constrangedora exposição na internet, ela consultou você para saber como retirar tal conteúdo do site de relacionamentos. Como Idalina deverá proceder para retirar seus dados desse site de relacionamentos?

Resolução da situação-problema

A remoção de conteúdos da internet pode ser feita de três maneiras distintas:

- Ação judicial.

- Notificação extrajudicial.

- Denúncia realizada no próprio site.

Primeiramente, Idalina deve verificar a existência de ferramenta dentro do próprio site com o objetivo de denunciar a ocorrência de ato ilícito.

Caso inexista tal ferramenta, ou caso seja feita a denúncia e o conteúdo continue on-line, ela deverá enviar notificação extrajudicial ao provedor de aplicação responsável pelo site onde o conteúdo encontra-se publicado, requerendo a remoção, sob pena de ingresso de ação judicial.

Se mesmo após o envio e recebimento da notificação extrajudicial o conteúdo continuar no site, Idalina deve propor ação judicial, requerendo a condenação tanto do autor do perfil falso, quanto do provedor de aplicação, nos termos do artigo 21 do MCI. Igualmente deverá ser requerida a revelação dos registros de aplicação referentes à criação e uso do perfil.

Faça valer a pena

1. Sem desconsiderar a dificuldade técnica de monitoramento prévio do conteúdo publicado, os tribunais brasileiros vinham apontando medidas que poderiam ser adotadas pelas empresas titulares das redes sociais para prevenir ou atenuar os danos causados às vítimas de atos ilícitos, de modo a evitar que tais provedores fossem objetivamente responsabilizados pelos atos praticados.
Assinale a alternativa que apresenta uma dessas medidas:
a) Envio de notificação eletrônica ao usuário autor do conteúdo ilícito, alertando-o sobre o recebimento de uma denúncia, porém sem remover o conteúdo.
b) Elaboração e divulgação de "cartilhas" com orientações às vítimas sobre como proceder.
c) Cobrança de valores pecuniários para remoção do conteúdo ilícito.
d) Criação de mecanismos efetivos para denunciar o conteúdo ilícito.
e) Guarda de dados inúteis para a identificação do usuário autor do ato ilícito.

2. O Marco Civil da Internet, de maneira simplificada, dividiu os provedores (serviços de administração de sistema autônomo) em duas categorias distintas, "provedores de conexão" e "provedores de aplicação". Todavia, a classificação dos provedores, ou sua distinção consoante à natureza dos serviços prestados, já era feita pela doutrina.
De acordo com a classificação feita por Marcel Leonardi, assinale a alternativa que apresenta uma espécie de provedor de serviços de internet que pode ser enquadrado na categoria de "provedor de conexão", conforme o Marco Civil da Internet:
a) Provedor de correio eletrônico.
b) Provedor de *backbone*.
c) Provedor de conteúdo.
d) Provedor de hospedagem.
e) Provedor de registro de site.

3. O Marco Civil da Internet veio como ferramenta para acabar com as discussões acerca da responsabilidade civil dos provedores de internet. Se antes da aprovação da citada lei víamos decisões judiciais que atribuíam a responsabilidade civil objetiva, hoje em dia elas são praticamente inexistentes. O artigo 19 positivou, em certa medida, a "responsabilidade _____" dos provedores, porém sua notificação deve ser feita de maneira _____, salvo para os casos de cenas de nudez e atos sexuais de caráter privado, nos termos do artigo 21 do MCI.

Preencha as lacunas com a única alternativa correta:

a) subsidiária – judicial.
b) solidária – extrajudicial.
c) condicionada – judicial.
d) civil – extrajudicial.
e) penal – extrajudicial.

Referências

ALEXY, Robert. **Teoria de los derechos fundamentales**. Madrid: Centro de Estudios Políticos y Constitucionales, 2002.

BACKBONE - História da Internet. **YouTube**, 3 mar. 2014. Disponível em: <https://www.youtube.com/watch?v=yhSUrTD3Q3I>. Acesso em: 14 jun. 2017.

BARROS. Suzana de Toledo. **O princípio da proporcionalidade e o controle da constitucionalidade das leis restritivas de direitos fundamentais**. 3. ed. Brasília: Brasília Jurídica, 2003.

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

BOBBIO, Norberto. **A era dos direitos. 19. reimpressão**. Tradução de Carlos Nelson Coutinho. Rio de Janeiro: Elsevier, 1992.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 5 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 16 jul. 2017.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 6 nov. 2018.

_____. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**, Brasília, 12 out. 1990.

_____. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, 11 jan. 2002.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. **Diário Oficial da União**, Brasília, 24 abr. 2014.

CANOTILHO, José Joaquim. **Direito Constitucional e Teoria da Constituição**. Coimbra: Almedina, 1988.

CASTRO, Mônica Neves Aguiar da Silva**. Honra, imagem, vida privada e intimidade, em colisão com outros direitos.** Rio de Janeiro: Renovar, 2002.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito e internet III**. São Paulo: Quartier Latin, 2015. Tomo I: Marco Civil da Internet (Lei n. 12.965/2014).

DECLARAÇÃO de direitos e responsabilidades. **Facebook**, 30 jan. 2015. Disponível em: <https://www.facebook.com/legal/terms>. Acesso em: 20 jun. 17.

DONEDA, Danilo. Princípios de proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito e internet III.** São Paulo: Quartier Latin, 2015. Tomo I: Marco Civil da Internet (Lei n. 12.965/2014).

ENTENDA o caso de Edward Snowden, que revelou espionagem dos EUA. G1, 14 fev. 2014. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 1º maio 2017.

FARIAS, Edilson Pereira de. **Colisão de direitos**: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. 2. ed. Porto Alegre: Sérgio Antônio Fabris, 2000.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**. 9. ed. v. 3. São Paulo: Saraiva, 2011.

HAIKAL, Victor Auilo. Direitos da personalidade na sociedade da informação. **DigitalRights**. cc, 6 mar. 2017. Disponível em: <http://digitalrights.cc/blog/2017/03/06/direitos-de-personalidade-na-sociedade-da-informacao/>. Acesso em: 13 maio 2017.

LEITE, Flávia Piva Almeida; MEYER-PFLUG, Samantha Ribeiro. A liberdade de expressão e o direito à privacidade no Marco Civil da Internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito e internet III**. São Paulo: Quartier Latin, 2015. Tomo I: Marco Civil da Internet (Lei n. 12.965/2014).

LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviços de internet**. São Paulo: Juarez de Oliveira, 2005.

MENEZES, Victor Hugo T. Mecanismos europeus de controle de dados na internet. **Jusbrasil**, 23 mar. 2017. Disponível em: <https://victorhugotmenezes.jusbrasil.com.br/artigos/441755140/mecanismos-europeus-de-controle-de-dados-na-internet>. Acesso em: 14 jun. 2017.

PARENTONI, Leonardo Netto. Direito ao esquecimento (Right to Oblivion). In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito e internet III**. São Paulo: Quartier Latin, 2015. Tomo I: Marco Civil da Internet (Lei n. 12.965/2014).

PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil**: introdução ao direito civil - Teoria Geral de Direito Civil - v. 1, 29. ed. 2007.

PINHEIRO, Patrícia Peck. Direito Digital. edição digital. São Paulo: Saraiva, 2013.

PODESTA, Fábio Henrique. Marco Civil da Internet e direitos da personalidade. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito e internet III**. São Paulo: Quartier Latin, 2015. Tomo I: Marco Civil da Internet (Lei n. 12.965/2014).

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Morais. Rio de Janeiro: Renovar, 2008.

RODRIGUES JUNIOR, Otávio Luiz. Direito de apagar dados e a decisão do tribunal europeu no caso Google Espanha. **Consultor Jurídico**, 21 maio 2014. Disponível em: <http://www.conjur.com.br/2014-mai-21/direito-apagar-dados-decisao-tribunal-europeu-google-espanha>. Acesso em: 7 jun. 2017.

ROHRMANN, Carlos Alberto. **Curso de Direito Virtual**. Belo Horizonte: Del Rey, 2005.

SZANIAWSKI, Elimar. **Direitos de personalidade e sua tutela**. São Paulo: Editora Revista dos Tribunais, 1993.

TEIXEIRA, Tarcísio. **Curso de direito e processo eletrônico**: doutrina, jurisprudência e prática. 3. ed. atual. ampl. São Paulo: Saraiva, 2015.

A propriedade na internet

Convite ao estudo

Caro aluno, conforme você se recorda, na última unidade estudamos as questões relacionadas aos direitos da personalidade aplicados dentro do contexto da internet. Estudamos principalmente os conflitos entre privacidade, liberdade de expressão, além da proteção dos dados pessoais face à ingerência de terceiros. Igualmente, analisamos a questão do direito ao esquecimento e a responsabilidade civil dos provedores de serviços de internet conforme o Marco Civil da Internet.

Nesta Unidade 3, iremos direcionar nossos estudos para a proteção dos bens imateriais dentro do meio eletrônico, ou seja, iremos deixar um pouco de lado os estudos sobre os direitos dos usuários, para estudar como se dá a proteção jurídica sobre os bens de propriedade deles, sobretudo aqueles de natureza incorpórea.

Para tanto, iremos considerar o seguinte contexto de aprendizagem: você, na condição de advogado e consultor jurídico, foi procurado por uma empresa *startup* do setor de tecnologia chamada Piper Comércio Eletrônico. Tal empresa tem por objetivo fornecer uma plataforma que facilita o processo de compra e venda de produtos usados através da internet, aproximando usuários compradores de usuários vendedores. Tal empresa o procurou para que você faça uma análise detalhada do modelo de negócio proposto, de modo a verificar a conformidade legal da plataforma desenvolvida com a legislação brasileira aplicável. Essa consultoria consiste na emissão de diversas opiniões legais a partir de dúvidas que irão surgir ao longo do processo de criação e desenvolvimento da empresa e de seus ativos digitais, tais como: é possível proteger

juridicamente uma ideia? Como é possível garantir o nome de domínio da empresa e como resolver eventual conflito? O direito de arrependimento é aplicável para compras na internet? Como se dá a contratação eletrônica entre site e usuário e quais os requisitos jurídicos de tal contratação?

A fim de respondermos esses e outros questionamentos, iremos estudar de uma forma geral, na Seção 3.1, a evolução do direito de propriedade e a proteção da informação por meio desse direito e suas eventuais adaptações. Na Seção 3.2, iremos estudar os conflitos entre nomes de domínio, métodos de solução, além dos desafios impostos por novas tecnologias ao direito autoral. Por fim, na Seção 3.3, iremos analisar os contratos eletrônicos e as normas aplicáveis a ele. Preparado? Vamos lá!

Seção 3.1

Direito da propriedade na internet

Diálogo aberto

Caro aluno, vamos trabalhar com a nossa situação-problema. Lembre-se de que você, na condição de advogado e consultor jurídico, foi procurado por uma empresa *startup* do setor de tecnologia chamada Piper Comércio Eletrônico. Ela pretende apresentar a plataforma digital para um grupo de investidores. Estes últimos, levando em consideração os riscos do investimento, pediram que fossem apresentadas diversas informações a respeito da plataforma, tais como estudos de mercado, trechos do código-fonte da plataforma, entre outros. Todavia, os sócios da empresa estão com receio de que tais informações sejam divulgadas para terceiros após tal apresentação. Diante dessa situação, seu cliente pediu sua opinião legal sobre como proteger juridicamente as informações reveladas sem comprometer a demonstração para o grupo de investidores. Qual sua opinião legal sobre essa situação? Tal proteção é garantida em lei? Existem outros mecanismos que visem proteger essas informações?

Para responder esses e outros questionamentos, iremos estudar, na presente seção, o processo evolutivo do direito de propriedade e o impacto que a tecnologia da informação teve sobre esse direito ao longo da história. Igualmente, iremos analisar alguns institutos advindos do direito de propriedade, cujo objetivo é justamente resguardar os ativos intangíveis de uma pessoa, tal qual o "segredo de comércio". Ao final, lembre-se de que os conteúdos estudados servirão de base para nosso parecer jurídico, ou seja, nosso produto final.

Não pode faltar

As novas tecnologias da informação têm apresentado diversos obstáculos a serem superados pelo direito, sobretudo aquele que resguarda os bens intangíveis, o direito da propriedade intelectual. Vários são os motivos, desde o acesso facilitado a esses bens no meio eletrônico, até a perfeição e rapidez com que cópias digitais são feitas, além do baixo custo desse procedimento de cópia.

Mas, antes de adentrarmos a questão da propriedade na internet, iremos traçar uma breve linha evolutiva do direito de propriedade, para vermos como chegamos ao estágio onde nos encontramos atualmente, em que a proteção da propriedade intelectual está muito mais focada nos meios tecnológicos do que no Direito propriamente dito.

O direito de propriedade é garantido no Brasil por força do disposto na Constituição Federal de 1988, especificamente no artigo 5º, caput e incisos XXII e XXIII, que assim dispõem:

> **Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:**
> **[...]**
> **XXII - é garantido o direito de propriedade;**
> **XXIII - a propriedade atenderá a sua função social; (BRASIL, 1988, art. 5º)**

Nesse aspecto, o Código Civil de 2002 também traz garantia ao direito de propriedade. Vamos entender um pouco mais sobre isso?

Assimile

O Código Civil de 2002 também traz a garantia ao direito de propriedade. Porém, seguindo a tradição do diploma de 1916, não define o direito de propriedade, apenas declina os direitos do proprietário, quais sejam, usar, gozar, dispor, reaver a coisa e reivindicá-la de quem quer que a possua ou detenha injustamente (BRASIL, 2002, art. 1.228).

A origem dos direitos intrínsecos à propriedade remonta desde ao Direito Romano, mais especificamente ao *Corpus Iuris Civilis* (CRETELLA JÚNIOR, 1995). O direito de propriedade no direito romano era visto como o "direito que liga o homem a uma coisa". Analisando esse conceito, percebemos como o direto de propriedade estava intimamente associado ao caráter tangível de uma coisa ou bem.

Assim, temos uma origem do direito de propriedade, que era voltado principalmente para os bens tangíveis, especialmente os bens imóveis. Por sua vez, o direito de propriedade sobre bens móveis, tornou-se mais elaborado ao longo da Idade Média e da Idade Moderna.

Foi somente há 300 anos que surgiu a proteção específica do direito da propriedade intelectual. O primeiro direito sobre um bem imaterial foi conferido por um decreto real em 1556, na Grã-Bretanha. Trata-se do copyright, que foi criado pouco após o advento da imprensa. Não podemos confundir o copyright com o "direito de autor", que nasceu na doutrina francesa e que possui aspectos filosóficos diversos, conforme veremos adiante.

A primeira lei inglesa que regulamentou o copyright foi o *Statute of Anne*, passada pelo parlamento britânico em 1710. Tal lei conferia aos criadores de uma obra o direto exclusivo sobre ela, por um prazo de 14 anos, renováveis por outro período de mais 14 anos.

Por sua vez, o direito continental foi conhecer a proteção legal dos direitos dos autores também no século XVIII. Conforme dito anteriormente, o governo revolucionário francês editou um decreto em 1791 dispondo sobre uma série de direitos dos autores. Porém, diferentemente da lei britânica, a lei francesa preocupava-se muito mais com os direitos morais dos autores, daí a distinção filosófica.

Dentro de nossa linha evolutiva, os direitos de propriedade intelectual foram positivados a partir do século XVIII, como já vimos. Mas isso não quer dizer que antes desse período obras literárias e invenções modernas ficavam desprotegidas. Em relação às primeiras, vimos que o decreto britânico de 1556 já garantia um direito que hoje conhecemos como copyright.

Pesquise mais

Saiba um pouco mais sobre propriedade intelectual em *O conceito de propriedade intelectual*. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/27573-27583-1-PB.pdf>. Acesso em: 16 jul. 2017.

Já em relação às invenções, sabe-se que as cidades-estados de Veneza e Florença, notadamente dedicadas ao comércio marítimo, possuíam leis que conferiam a um inventor um privilégio ou monopólio sobre sua invenção pelo prazo de dez anos (RORHMANN, 2015). Trata-se de direto semelhante ao direito de patentes, como temos hoje.

Essa brevíssima linha evolutiva que vimos demonstra que a proteção jurídica sobre a propriedade tende a ser tão mais elaborada conforme a época e o tipo de propriedade que tem maior importância prática e econômica para uma determinada sociedade em um determinado

período da história.

Atualmente, vemos um grande crescimento da propriedade intelectual para o direito e para a economia, seja em razão da indústria do entretenimento, havendo preocupação com a pirataria de conteúdos digitais, como séries, músicas e jogos eletrônicos, além de programas de computador, seja através da indústria moderna, que cada vez mais necessita de proteção patentária para suas invenções.

Pesquise mais

Observa-se, ainda, o aumento da importância da informação na economia. É consenso entre diversos especialistas que dados pessoais representam o novo "petróleo" da internet. Novas tecnologias da informação baseadas nos fenômenos do "Big Data" e da "Internet das Coisas", são cada vez mais comuns e valiosas, daí a necessidade cada vez maior de proteção do direto de propriedade sobre as bases de dados. Para saber mais sobre o "Big Data" e a "Internet das Coisas", sugerimos a leitura do artigo *Big Data* e *Internet das Coisas* serão motores de uma nova economia. Disponível em: <http://computerworld.com.br/big-data-e-internet-das-coisas-serao-motores-de-uma-nova-economia>. Acesso em: 5 jul. 2017.

Meu caro aluno, depois de ver os conceitos sobre direito de propriedade, vamos agora analisar as formas de adaptação que ele vive em relação à proteção dos bens intangíveis, focando os desafios trazidos pela virtualização da propriedade intelectual.

A importância da informação como uma verdadeira "mercadoria" do mundo virtual é evidenciada, principalmente, pelos serviços de busca na internet. A informação, independentemente do suporte físico em que se encontra, é sempre um bem não dotado de existência física, ou seja, é essencialmente imaterial, uma vez que se refere a uma ideia ou ao acréscimo de um certo conhecimento já existente (ROHRMANN, 2015).

A proteção da informação se dará, primordialmente, pelo direito da propriedade intelectual ou por algum instituto intrínseco a este, como as normas que regulam a concorrência desleal. Tal proteção é algo extremamente complexo do ponto de vista técnico e jurídico, tendo em vista a necessidade de se fazer adaptações no instituto da propriedade, de modo a torná-lo mais eficiente no tocante ao

atendimento das garantias de uso exclusivo pelos titulares desses bens incorpóreos.

Uma forma muito interessante de proteção que foi evoluindo ao longo dos anos para atender às necessidades de proteção à informação intangível, porém economicamente apreciável, é o instituto dos "segredos de comércio".

Não se pode negar a existência de determinadas informações empresariais sigilosas dotadas de considerável valor econômico para os setores da indústria e do comércio. A título de exemplo, podemos citar a fórmula da Coca-Cola ou o algoritmo de buscas do Google.

Assimile

Conforme o professor Denis Borges Barbosa, o segredo de comércio, também chamado de "segredo de empresa", pode ser definido como uma "informação, técnica ou não, caracterizada por escassez suficiente para lhe dotar de valor competitivo num determinado mercado" (BARBOSA, 2008, p. 1).

Quando pensamos na ferramenta de proteção jurídica com objetivo de proteger informações sigilosas e valiosas para uma empresa, pensamos primeiramente no instituto da patente, pois este confere um monopólio sobre aquele determinado bem ou informação. Todavia, ela pode não ser uma solução adequada para garantir o domínio em determinado mercado. Isso porque o direito patentário exige a posterior publicação das informações protegidas em troca da garantia do monopólio temporário.

Assim é que surgiu o instituto jurídico dos "segredos de comércio" (*Trade Secrets*), que tem sua origem no sistema de *Common Law* e que, atualmente, exerce papel fundamental na proteção jurídica da propriedade.

O objeto de proteção jurídica desse instituto é justamente a informação sigilosa, o segredo (que não precisa ser absoluto, podendo ter um pequeno descortinamento para alguns empregados ou empresas fornecedoras) economicamente apreciável. A título de exemplo, qualquer fórmula, padrão, compilação, programa, dispositivo, método, técnica ou processo sigilosos e valiosos poderiam merecer, em tese, proteção jurídica (ROHRMANN, 2015).

Exemplificando

Na reportagem *5 segredos industriais guardados a sete chaves*. Disponível em: <https://www.tecmundo.com.br/curiosidade/18707-5-segredos-industriais-guardados-a-sete-chaves.htm>. Acesso em: 16 jul. 2017, temos exemplos de alguns dos segredos mais famosos, atualmente, no mundo empresarial. Você conhece mais algum?

Por sua vez, a legislação brasileira não confere, ainda, direito de propriedade ao titular do segredo comercial. Todavia, a Lei nº 9.279 de 1996 (Lei de Propriedade Industrial) regula, em seu artigo 195, os chamados "crimes de concorrência desleal". Alguns desses tipos penais cuidam de uma proteção jurídica semelhante àquela dispensada ao *Trade Secret* norte-americano, conforme se depreende da leitura do artigo citado:

> Art. 195. Comete crime de concorrência desleal quem:
> [...]
> XI - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;
> XII - divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude; ou
> [...]
> XIV - divulga, explora ou utiliza-se, sem autorização, de resultados de testes ou outros dados não divulgados, cuja elaboração envolva esforço considerável e que tenham sido apresentados a entidades governamentais como condição para aprovar a comercialização de produtos.
> Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa. (BRASIL, 1996, art. 195)

Podemos considerar essas normas contidas no artigo 195 como as principais que servem de referência para a proteção dos segredos de comércio. Cumpre destacar a pena fixada pelo legislador para um crime cada vez mais grave em um contexto de economia digital como o que vivemos.

Algumas críticas à legislação brasileira residem no fato de que ela não garante um direito de propriedade, por assim dizer, ao segredo comercial. Trata-se de verdadeira adaptação a um instituto que vem ganhando importância e destaque, pois assegura a tranquilidade do empresário em relação à proteção de seu negócio.

Por um lado, conferir um direito de propriedade sobre um segredo comercial é favorável às pequenas empresas, que não possuem capital para investir na segurança da informação sigilosa. Por outro lado, tal garantia pode representar um obstáculo ao desenvolvimento da ciência e da tecnologia, pois impediria a troca de ideias e informações, algo fundamental ao desenvolvimento tecnológico de um país ou região.

Admitir a possibilidade de se estender o direito de propriedade aos segredos de comércio e, naturalmente, à informação, atrai a necessidade de discutirmos também a possibilidade de se aplicar a proteção possessória aos arquivos digitais – tradicionalmente, o instituto da proteção possessória aos bens móveis. Mas o que é um bem móvel?

O Código Civil de 2002 inovou ao estender o conceito de bem móvel às "energias que tenham valor econômico" (BRASIL, 2002, art. 82 e 83). Nesse sentido, temos que os arquivos digitais de computador são "energia armazenada", seja em meio magnético (ex.: discos rígidos), seja em meio ótico (ex.: CDs) (ROHRMANN, 2015).

Não iremos aqui discutir a proteção do direto de propriedade intelectual sobre os conteúdos desses arquivos digitais, pois eles podem conter um programa de computador ou uma obra musical em seu formato digital, os quais são protegidos por direito autoral. Assim, para analisarmos a proteção possessória sobre os arquivos digitais propriamente ditos, temos que antes analisar o conceito de direito real.

Para Washington de Barros Monteiro, o direito real pode ser conceituado como uma relação jurídica em virtude da qual o titular

pode tirar da coisa, de modo exclusivo e contra todos, as utilidades que ela é capaz de produzir (MONTEIRO, 1998).

Destarte, temos que o direito sobre os arquivos digitais poderia ser considerado um direito real, haja vista possibilidade de o titular tirar as utilidades, por exemplo, de um determinado website, o que, sob a garantia jurídica, há de lhe ser deferida de forma exclusiva. Assim, poderíamos aplicar a proteção possessória para os arquivos digitais de um website em certos casos de turbações à posse no meio eletrônico.

Exemplificando

Podemos citar alguns exemplos práticos de situações que configurariam essa turbação possessória: caso alguém realizasse cópias excessivas de dados contidos em um website. A turbação possessória residiria no fato de que os computadores que hospedam o website estariam sendo sobrecarregados pelo excesso de acessos oriundos de terceiro, com uma consequente queda no desempenho do site, o que poderia ser prejudicial caso se tratasse, por exemplo, de um site de empresa de comércio eletrônico. Como não há, em princípio, proteção de direitos autorais sobre os dados copiados, o titular do website poderia conseguir uma liminar possessória para impedir que esse terceiro acessasse o website.

A questão é certamente nova, não havendo decisões sobre a aplicabilidade das tutelas possessórias sobre arquivos digitais. Mas, como vimos, certamente essa possibilidade apresenta-se viável.

Reflita

Na sua opinião, seria possível aplicar os institutos da tutela possessória aos arquivos digitais? Será que a legislação brasileira sobre o tema permite interpretação tão extensiva?

Chegamos ao fim de mais uma apresentação de importantes conceitos para que você possa solucionar a situação-problema proposta. Concluindo, temos que o direito de propriedade foi evoluindo conforme a importância que determinada sociedade conferia aos bens imateriais. Atualmente, em um cenário de economia digital, temos que tal instituto se apresenta importante para resguardar os ativos de várias empresas. Apesar da legislação brasileira não conferir proteção específica a dados e informações por meio do direito de propriedade, temos que este sofreu algumas adaptações, que podem ser usadas para resguardar ativos intangíveis, tais como a

doutrina dos segredos de comércio, concorrência desleal ou, ainda, tutelas possessórias sobre arquivos digitais.

Sem medo de errar

Vamos relembrar nossa situação-problema? Após sua contratação, a empresa pediu sua opinião legal sobre como proteger informações confidenciais sobre o próprio negócio desenvolvido por ela, porém sem comprometer a demonstração a ser realizada aos potenciais investidores. Qual sua opinião legal sobre essa situação? Tal proteção é garantida em lei? Existem outros mecanismos que visam proteger essas informações?

Iremos responder tais questões na forma de uma opinião legal, ok?

Primeiramente, devemos verificar qual a espécie de informação que os investidores pediram que fosse revelada. Nesse sentido, lista de clientes, estudos de mercado, trechos de códigos de programação, entre outros, possuem considerável valor econômico, pois foram investidos recursos financeiros na produção dessas informações. Além disso, tais informações são, a princípio, sigilosas, pois proporcionam uma vantagem competitiva da empresa sobre seus concorrentes.

Dessa maneira, tais informações devem ser protegidas juridicamente. Mas como?

Quando pensamos na ferramenta de proteção jurídica com objetivo de proteger informações sigilosas e valiosas para uma empresa, pensamos primeiramente no instituto da patente, pois confere um monopólio sobre aquele determinado bem ou informação. Todavia, essa pode não ser uma boa solução para seu cliente, porque o direito patentário exige a posterior publicação das informações protegidas em troca da garantia do monopólio temporário. Igualmente, tais informações não são passíveis de concessão de patente, nos termos da Lei de Propriedade Industrial.

Uma forma alternativa de proteção de informações, advinda do próprio direito de propriedade, é o instituto do segredo de comércio.

O objeto de proteção jurídica desse instituto é justamente a informação sigilosa, o segredo (que não precisa ser absoluto, podendo ter um pequeno descortinamento para alguns empregados ou empresas fornecedoras) economicamente apreciável.

Entretanto, a legislação brasileira não confere, ainda, direito de propriedade ao titular do segredo comercial. Não obstante, a Lei nº 9.279 de 1996 (Lei de Propriedade Industrial) regula, em seu artigo

195, os chamados "crimes de concorrência desleal". Alguns desses tipos penais cuidam de uma proteção jurídica semelhante àquela dispensada ao segredo de comércio.

Outra forma viável de proteção de tais informações é o próprio direito contratual.

Assim, a empresa cliente poderia apresentar um "termo de confidencialidade" (*Non Disclosure Agreement* – NDA) para os investidores, estabelecendo cláusulas que determinam o pagamento de multa compensatório em caso de vazamento de informações confidenciais.

Avançando na prática

A tutela possessória sobre arquivos digitais

Descrição da situação-problema

Considere que o site de seu cliente foi devidamente lançado no mercado, apresentando grande popularidade e alcançando altos valores de vendas diárias. Em certa ocasião, a equipe técnica do site verifica que um hacker está fazendo cópias excessivas dos dados contidos no website, por meio de um programa do tipo *Crawler* ou *Spider*, que fazem a coleta massiva e automatizada de dados do site. Pergunta-se: é juridicamente viável requerer que esse hacker interrompa suas atividades por meio de uma liminar possessória?

Resolução da situação-problema

A utilização dos institutos da tutela possessória demanda, necessariamente, a existência de turbação na posse do titular de um bem, seja este tangível ou intangível. Se considerarmos a situação narrada, temos que a turbação possessória residiria no fato de que os computadores que hospedam o website da empresa estariam sendo sobrecarregados pelo excesso de acessos oriundos das atividades do hacker. Consequentemente, verifica-se uma queda no desempenho do site, o que poderia ser prejudicial ao cliente, por se tratar de um site de empresa de comércio eletrônico.

Como não há, a princípio, proteção de direitos autorais sobre os dados copiados, o titular do website, seu cliente, poderia conseguir uma liminar possessória para impedir que esse terceiro acessasse o website.

Faça valer a pena

1. O direito de propriedade, no Direito Romano, era visto como "o direito que liga o homem a uma coisa" e surgiu inicialmente para proteger os direitos sobre bens imóveis e, posteriormente, os bens incorpóreos (CRETELLA JÚNIOR, 1995).

Analisando o texto, assinale a única alternativa correta que contém um exemplo de proteção a bem imaterial.

a) Direito sobre um computador que contém uma obra literária.
b) Direito sobre a informação contida em um site.
c) Direito sobre um livro de autor renomado.
d) Direito sobre um aparelho DVD que reproduz filmes.
e) Direito sobre um produto adquirido pela internet.

2. A origem dos direitos de propriedade vem desde o Direito Romano, quando o imperador Justiniano criou uma legislação que visava atender às demandas da época. Nesse período, o direito de propriedade era considerado direito real e absoluto.

O texto se refere a qual legislação?

a) Código Civil.
b) Código de Hamurabi.
c) *Corpus iuris civilis.*
d) Lei de Talião.
e) Constituição Federal.

3. Atualmente, temos a proteção jurídica do(a) chamado(a) _____, instituto oriundo do direito _____, que visa resguardar o sigilo de fórmulas, métodos de organização de informação, enfim, quaisquer informações relevantes de uma empresa e que tenha valor comercial.

Assinale a alternativa que preenche corretamente as lacunas do texto.

a) Segredo de comércio; norte-americano.
b) Marca; inglês.
c) Nome empresarial; alemão.
d) *Common Law*; norte-americano.
e) Copyright; britânico.

Seção 3.2

Marcas registradas, nomes de domínio e direitos autorais

Diálogo aberto

Novamente, saudações, aluno! Conforme vimos na seção anterior, nosso contexto de aprendizagem traz uma situação hipotética em que seu cliente, uma empresa *startup* chamada Piper Comércio Eletrônico, pretende fornecer a seus usuários uma plataforma que facilita o processo de compra e venda de produtos usados por meio da internet.

Para tanto, a empresa pretende registrar o nome de domínio www.piper.com.br. Porém, ele já se encontra registrado em nome de uma outra pessoa jurídica. Atualmente, o site vinculado ao nome de domínio citado é utilizado para venda de produtos destinados ao consumo de substâncias ilícitas, especificamente maconha. Na condição de advogado e consultor jurídico da Piper Comércio Eletrônico, qual seria seu conselho jurídico, no sentido de orientar seu cliente se seria possível pedir a transferência desse nome de domínio? Quais os mecanismos de resolução de conflitos disponíveis para realização de tal pedido? Seria possível resolver pela via extrajudicial? Ou teríamos que recorrer à via judicial? Lembre-se de que, ao final, iremos elaborar um parecer jurídico de modo a sanar as dúvidas do nosso cliente.

Para resolver a situação-problema proposta, iremos estudar o conceito de nomes de domínio, o sistema de registro de nomes de domínio no Brasil, os órgãos encarregados desse registro, os mecanismos disponíveis aos usuários para eventual resolução de conflito entre nomes de domínio, marcas registradas, nomes empresariais e nomes artísticos. De maneira complementar, iremos analisar também os desafios impostos pelas novas tecnologias aos direitos autorais, considerados uma vertente do direito de propriedade intelectual, com foco nas recentes decisões envolvendo as tecnologias *streaming*.

Não pode faltar

Na última seção, estudamos questões relacionadas ao direito de propriedade na internet. Nesta seção, aprofundaremos tais estudos, analisando a proteção jurídica sobre nomes de domínio, marcas

e direitos autorais, sendo que esses dois últimos termos serão contextualizados conforme as inovações trazidas pela rede mundial de computadores.

Conforme vimos no início dos nossos estudos, a internet opera sobre uma tecnologia da informação que se utiliza da troca de pacote de dados entre computadores conectados a um emaranhado de redes, em escala global. Para que haja uma troca efetiva de pacotes de dados, é necessária a correta identificação dos computadores que atuam como remetentes, destinatários e intermediários desses pacotes. Para tanto, utilizamos os nomes de domínio.

Assimile

Nomes de domínio são expressões utilizadas para localizar e identificar conjuntos de computadores e serviços de internet, a fim de evitar ter de localizá-los por meio de seus numerais identificadores. Vale dizer que os nomes de domínio servem para designar o endereço eletrônico de um website.

Um nome de domínio está diretamente relacionado com o endereço IP (protocolo de internet) de um computador, ou seja, ao procurar por um nome de domínio ou endereço de uma página na internet, estamos na verdade buscando o endereço de um determinado computador. A memorização de um nome de domínio é mais fácil que a memorização do número IP atribuído àquele computador.

Exemplificando

É muito mais fácil acessarmos e memorizarmos o website da empresa Kroton por meio de seu nome de domínio www.kroton.com.br, do que de seu endereço IP (187.86.214.62).

Você consegue pensar em mais algum website?

As funções do nome de domínio são basicamente duas: possibilitar a conexão de um usuário com o conteúdo de um website e identificar o titular daquele endereço eletrônico, através de seu nome (pessoal ou empresarial) ou marca, por exemplo.

Para que se torne o titular de um determinado nome de domínio, o usuário precisa fazer o registro desse nome. Em âmbito brasileiro, os registros dos nomes de domínio com extensão ".br" são de responsabilidade do Registro.br, órgão diretamente ligado ao Núcleo

de Informação e Coordenação do Ponto BR (Nic.br), que por sua vez é vinculado ao Comitê Gestor da Internet (CGI), que estudamos na Unidade 1 deste curso.

Entre suas diversas atribuições, o Nic.br é responsável pelo registro e pela manutenção dos domínios que se utilizam da extensão ".br", além da distribuição de endereços IP no país. A principal norma que rege as regras para registro de um nome de domínio é a Resolução nº 008 de 2008 do CGI.

De acordo com o artigo 1º dessa resolução, um nome de domínio será concedido ao primeiro requerente que satisfizer as exigências para o registro de tal domínio, devendo o requerente respeitar os direitos de terceiro, até mesmo de propriedade intelectual, sendo ainda vedada a utilização de expressões que induzam terceiros a erro ou que representem conceitos predefinidos na rede, de palavras de baixo calão ou abusivas ou, ainda, que simbolizem siglas de estados, ministérios, entre outras vedações, assim como o registro para prática de atividades ilícitas.

Trata-se da regra que ficou conhecida como "*first come, first served*". Dessa forma, o interessado, ao registrar um nome de domínio, poderá registrar um nome que represente uma marca, nome empresarial, nome ou apelido de pessoa famosa, etc., cuja titularidade não possua. Os problemas jurídicos ocorrem justamente quando o nome de domínio conflita com uma marca ou nome.

Podemos conceituar uma "marca" como um sinal colocado em um produto ou serviço para que este seja identificado e distinguido, podendo ser uma palavra, símbolo, expressão, desenho, emblema ou outras representações gráficas. Ao registrar uma marca, seu titular tem uma série de direitos garantidos sob a ótica da Lei nº 9.279 de 1996 (Lei de Propriedade Industrial).

Bem, caro aluno, a ideia é não aprofundar nossos estudos sobre os direitos marcários, tendo em vista que este é um curso de Direito Eletrônico, e não de Direito de Propriedade Intelectual. Iremos analisar as situações onde uma marca conflita com um nome de domínio.

Como vimos, a norma estabelecida pelo Comitê Gestor da Internet (CGI) não exige a apresentação de qualquer comprovante de titularidade da marca para seu registro como nome de domínio. Igualmente, não existe nenhum tipo de consulta às bases de dados do Instituto Nacional da Propriedade Intelectual (INPI). Basta o nome

de domínio estar livre no servidor do órgão registrador, para que sua titularidade e uso na rede sejam autorizados.

Assim, um requerente poderá, de má-fé, utilizar-se de marca de titularidade de terceiro para registrar um nome de domínio, induzindo terceiros a erro, o que pode configurar tanto fraude quanto crime de concorrência desleal.

Essa situação conflituosa pode ocorrer também em relação aos nomes empresariais e nomes artísticos, com valor comercial. Mesmo que uma pessoa ou empresa não tenha uma marca registrada, seu nome empresarial (designação que identifica um empresário ou estabelecimento comercial) poderá ser protegido contra a má-fé de terceiros, especialmente sob a égide da concorrência desleal. Por sua vez, pessoas famosas, cujo nome artístico possuem reconhecido valor comercial, também podem ser protegidos, principalmente pelas normas do Código Civil que regulam os direitos da personalidade (artigos 16 a 19).

Exemplificando

Podemos citar os casos envolvendo o registro de nomes de domínio muito semelhantes, com intuito de atrair (e confundir) a clientela da concorrência. "A 9ª Câmara Cível do Tribunal de Justiça do Rio Grande do Sul (TJRS) inclusive cancelou o registro de um domínio de internet de empresa por ser semelhante na grafia de outro mais antigo, de competidor do mesmo ramo. Para o TJRS, o uso do domínio parecido com o original configura a prática de concorrência desleal" (TRIBUNAL, 2009, [s.p.]).

Havendo conflito entre o titular de um nome de domínio e o titular de uma marca, nome empresarial ou nome artístico, poderão as partes resolver tal problema por meio de arbitragem ou com a intervenção do Poder Judiciário. Todavia, antes de adentrarmos nos estudos sobre os mecanismos de solução de conflitos entre nomes de domínio, é necessário fazermos uma ressalva em relação aos nomes de domínio internacionais, ou seja, aqueles que não possuem a terminação ".br".

Nesse sentido, a Internet Corporation for Assigned Names and Numbers (ICANN), entidade privada sem fins lucrativos responsável pela coordenação e gerência da atribuição de nomes de domínio ao redor do mundo, criou um mecanismo de arbitragem internacional – o Uniform Dispute Resolution Policy (UDRP) – que se apresenta,

até mesmo, como solução de cunho obrigatório para todos aqueles que registram nomes de domínio não associados a determinado país, ou seja, "nomes de domínios internacionais". A arbitragem da ICANN ocorre no âmbito da Organização Mundial da Propriedade Intelectual (OMPI), em Genebra, na Suíça.

As decisões arbitrais são, normalmente, favoráveis aos titulares das marcas registradas no sentido de evitarem confusão e diluição no ambiente virtual. Entre tais decisões, podemos citar os casos envolvendo os domínios "globo.com" e "embratel.com". Em ambos, os laudos arbitrais foram favoráveis às empresas brasileiras, haja vista a importância das marcas no território nacional.

Por sua vez, os conflitos entre nomes de domínio nacionais, ou seja, aqueles com terminação ".br", podem ser resolvidos tanto pela via administrativa, quanto pela via judicial.

No primeiro caso, temos que o Comitê Gestor da Internet (CGI) implementou, em outubro de 2010, o chamado Sistema de Administração de Conflitos de Internet, ou SACI-Adm. Este, por sua vez, tem caráter facultativo, sendo que uma pessoa, ao registrar um domínio com a extensão ".br", adere automaticamente a esse sistema arbitral, por força do contrato firmado entre a entidade registradora, o Registro.br e o requerente de um nome de domínio.

Os procedimentos do SACI-Adm limitam-se ao cancelamento e à transferência do domínio em disputa, sendo que quaisquer pedidos de indenização por perdas e danos (materiais e morais) deverão ser levados ao crivo do Poder Judiciário.

Em todos os casos, deve a parte que iniciou o processo (arbitral ou judicial) demonstrar a má-fé no uso do domínio. Para fins de comprovação dos indícios dessa má-fé, deverá restar demonstrado, conforme aborda Pinheiro:

> (i) ter o titular registrado o nome de domínio com objetivo de vendê-lo, alugá-lo ou transferi-lo para o reclamante ou para terceiros;
> (ii) ter o titular registrado no nome de domínio para impedir que o reclamante o utilize como nome de domínio correspondente;
> (iii) ter o titular registrado o nome de domínio com objetivo de prejudicar a atividade comercial do reclamante;

> (iv) ter o titular utilizado o nome de domínio para tentar atrair, intencionalmente e com objetivo de lucro, usuários da internet para seu website ou outro endereço de rede, causando assim confusão. (PINHEIRO, 2015, p. 325)

No tocante à utilização do nome de pessoas naturais como nomes de domínio, temos que também há de se respeitar a vontade da pessoa em preservar seu nome, especialmente em se tratando de pessoas públicas ou famosas. Trata-se de proteção dos direitos da personalidade dentro da sistemática do Código Civil Brasileiro, especificamente em seus artigos 16 a 19.

Assim, nos casos em que alguém tente fazer o registro de um nome de domínio contendo o nome de terceiro, a princípio, este terceiro tem direito de cancelar o registro. É claro que o princípio da boa-fé deve ser observado quando do registro do nome de domínio. A exceção residiria justamente nos casos de homônimos. Entretanto, o registro com nomes de famosos ou políticos em época de eleição são normalmente dotados de má-fé, uma vez que o desejo é poder lucrar com a transferência do nome de domínio (ROHRMANN, 2015).

A boa-fé, ou pelo menos a ausência de má-fé, apresenta-se como verdadeira bússola para orientar a decisão de árbitros ou magistrados nos casos envolvendo conflitos entre direitos fundamentais, sendo que, caso respeitada, deve-se adotar a regra geral do "*first come, first served*".

Outro aspecto relevante do direito de propriedade intelectual que merece um estudo mais aprofundado pelo Direito Eletrônico refere-se aos desafios impostos aos direitos autorais pelas novas tecnologias.

Desde o advento da tecnologia de MP3, que convertia arquivos de áudio em arquivos digitais, autores, compositores e associações de representação e arrecadação de royalties ficaram preocupados com os possíveis impactos sobre a economia do entretenimento. Ao longo dos anos, antigos paradigmas foram quebrados, e a venda de CDs, por exemplo, foi diminuindo em ritmo acelerado.

Novos modelos de negócio foram aparecendo, sendo que as novas mídias digitais se tornaram a principal fonte de divulgação dos trabalhos dos artistas. Igualmente, eles passaram a arrecadar mais com shows e produções presenciais do que com a venda de discos ou arquivos de áudio. Uma dessas tecnologias que impactaram profundamente a forma como conteúdos protegidos por direitos

autorais são divulgados e, consequentemente, executados, é justamente o *streaming*.

Tal tecnologia propicia aos usuários a possibilidade de, por meio de conexão com a internet, ouvir músicas, assistir a vídeos, filmes e outros programas, que eram normalmente transmitidos no rádio e na televisão. Essa modalidade possibilita ao usuário a interação com qualquer dispositivo que disponha de acesso à internet (celulares, tablets, etc.) sem restrições de locais. No entanto, a legislação brasileira, especificamente a Lei de Direitos Autorais (Lei nº 9.610/98), não faz qualquer menção direta ao *streaming* de conteúdos protegidos.

Exemplificando

A tecnologia *streaming* vem, cada vez mais, dominando os mercados de reprodução de conteúdo de áudio e vídeo. A título de exemplo de plataformas on-line que fazem uso desse tipo de tecnologia, podemos citar, entre outras: Netflix, Spotify, Social Comics e Crunchyrool. E você, consegue pensar em mais alguma?

Nesse sentido, temos que o artigo 68 da Lei de Direitos Autorais determina que não podem ser utilizadas em execução pública ou representação: obras teatrais, composições musicais ou lítero-musicais e fonogramas sem prévia e expressa autorização do autor (BRASIL, 1998, art. 68).

O termo "execução pública" é definido no mesmo artigo como a utilização de composições musicais ou lítero-musicais, mediante a participação de artistas, remunerados ou não, ou a utilização de fonogramas e obras audiovisuais em locais de frequência coletiva, por quaisquer processos, inclusive a radiodifusão ou transmissão por qualquer modalidade e a exibição cinematográfica.

Tradicionalmente, os royalties cobrados pela execução pública de conteúdos protegidos por direitos autorais ficam a cargo do Escritório Central de Arrecadação e Distribuição (ECAD). O ECAD, entende que a transmissão de conteúdos via *streaming* gerava a obrigação de pagamento de royalties por parte dos provedores de serviços de internet. Estes, por sua vez, entendiam que tal cobrança era indevida, tendo em vista que o *streaming* não poderia ser considerado uma modalidade de execução pública. Coube ao Poder Judiciário pacificar o tema.

No Recurso Especial nº 1.559.264, a 2ª Seção do Superior Tribunal de Justiça deu provimento ao recurso do ECAD e decidiu que é legítima a arrecadação dos direitos autorais por este órgão nas transmissões musicais pela internet, via *streaming*.

Pesquise mais

Um breve resumo da decisão citada e o conteúdo do voto do relator, ministro Villas Bôas Cueva, encontra-se em:

SERVIÇOS de streaming de músicas deverão pagar direitos autorais ao Ecad. **STJ**, 10 ago. 2017. Disponível em: <http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunica%C3%A7%C3%A3o/noticias/Not%C3%ADcias/Servi%C3%A7os-de-streaming-de-m%C3%BAsicas-dever%C3%A3o-pagar-direitos-autorais-ao-Ecad>. Acesso em: 13 ago. 2017.

Em sua decisão, os ministros ainda fizeram a diferenciação entre "*simulcasting*" (retransmissão simultânea do conteúdo em outro meio de comunicação) e "*webcasting*" (retransmissão que oferece ao usuário a possibilidade de interferir na ordem da transmissão, como, por exemplo, na criação de listas de reprodução de músicas). Entretanto, entenderam que, independentemente da forma como o *streaming* é realizado, são devidos os direitos autorais pela execução da obra.

No entanto, essa decisão pode ser interpretada como um tanto quanto equivocada. Primeiramente, porque a divisão das modalidades de *streaming* em *simulcasting* e *webcasting* não é a mais correta, uma vez que o *webcasting* pode ser considerado gênero ao qual o *simulcasting* pertence. O ideal seria apresentar os conceitos de *live streaming* (o que conhecemos como "ao vivo") e *on demand* (programação por solicitação do espectador).

A Lei de Direitos Autorais dispõe que é considerada execução pública a transmissão por qualquer modalidade. O *live streaming* apresenta a simultaneidade necessária para a caracterização da execução pública. Por outro lado, no *streaming on demand* não se verifica tal simultaneidade, uma vez que cada pessoa recebe aquela obra no momento em que deseja, não havendo, assim, um conjunto de espectadores. A obra é simplesmente colocada à disposição do público na internet (GRADO, [2014b]).

Nesse sentido, o fato de algo estar disponível na internet não implica necessariamente em uma comunicação ou execução ao público, o que ensejaria o pagamento de direitos autorais ao ECAD. Trata-se de assunto delicado, sobretudo em razão do seu aspecto técnico e jurídico. Em que pese a decisão do STJ não ter sido a mais acertada, o tema foi colocado em voga, gerando a necessária discussão para o avanço na legislação.

Reflita

Na sua opinião, o Superior Tribunal de Justiça agiu corretamente ao definir as transmissões por meio de tecnologia *streaming* como verdadeiras execuções públicas? Em sua reflexão, pondere o aspecto técnico da decisão e a proteção dos direitos dos autores.

Concluindo, vimos que o direito de propriedade é igualmente resguardado na internet. Para tanto, o registro de nomes de domínio deve seguir uma série de regras que visam evitar o abuso dos usuários e eventuais violações aos direitos sobre marcas registradas, nomes empresariais e nomes artísticos. Ademais, verificamos uma preocupação na doutrina e na jurisprudência de proteger os direitos autorais diante do advento de novas tecnologias, como o *streaming* de conteúdos protegidos por meio da internet.

Sem medo de errar

Retomando nossa situação-problema, temos que sua cliente, a empresa Piper Comércio Eletrônico, pretende registrar o nome de domínio www.piper.com.br, que já se encontra registrado em nome de uma outra pessoa jurídica. Atualmente, o site vinculado ao nome de domínio citado é utilizado para venda de produtos destinados ao consumo de substâncias ilícitas, especificamente maconha. você, como advogado e consultor jurídico da Piper Comércio Eletrônico, deverá dar a orientação correta a seu cliente. Será que seria possível pedir a transferência desse nome de domínio? Quais os mecanismos de resolução de conflitos disponíveis para realização de tal pedido? Seria possível resolver pela via extrajudicial? Ou teríamos que recorrer à via judicial?

Lembre-se de que sua opinião legal deverá constar no parecer sugerido no início da unidade.

Conforme estudamos ao longo desta seção, o registro dos nomes de domínio com extensão ".br" são de responsabilidade do Registro.br, órgão diretamente ligado ao Núcleo de Informação e Coordenação do Ponto BR (Nic.br), que por sua vez é vinculado ao Comitê Gestor da Internet (CGI). Vejamos o que diz a referida norma, adaptando nossa análise ao formato de parecer.

REGULAMENTAÇÃO DOS NOMES DE DOMÍNIO NO BRASIL E SOLUÇÃO DE CONFLITOS

De acordo com o artigo 1º da Resolução nº 008 de 2008 do CGI, um nome de domínio será concedido ao primeiro requerente que satisfizer as exigências para o registro. Trata-se da regra que ficou conhecida como "*first come, first served*".

Todavia, tal requerente deve respeitar os direitos de terceiro, inclusive de propriedade intelectual, sendo ainda vedada a utilização de expressões que induzam terceiros a erro, que representem conceitos predefinidos na rede, de palavras de baixo calão ou abusivas ou ainda que simbolizem siglas de estados, ministérios, entre outras vedações, como o registro para a prática de atividades ilícitas.

Considerando que a venda de substâncias tóxicas, tal como a maconha, é vedada na legislação brasileira, temos que a criação de um website com o fim específico de vender tal substância, aliada ao registro de nome de domínio que utiliza a denominação empresarial ou marca de uma outra empresa, é inicialmente vedado, nos termos da citada Resolução nº 008 do CGI.

SUGESTÃO DE MEDIDAS JURÍDICAS A SEREM TOMADAS

De modo a resguardar os direitos e de requerer a transferência do nome de domínio www.piper.com.br, sugerimos a instauração de procedimento arbitral e, subsidiariamente, processo judicial. No primeiro caso, poderá ser utilizado o sistema SACI-Adm, devendo ser provada a ilicitude, abuso ou má-fé do usuário que requereu o registro. Igualmente, é possível intentar ação judicial com o mesmo propósito, sendo que o objeto de prova é exatamente o mesmo.

Avançando na prática

Direitos autorais e os modelos de rádio on-line

Descrição da situação-problema

Leôncio, ex-locutor de uma rádio, decidiu largar seu emprego e se dedicar a desenvolver um site cujo objetivo principal é ser uma verdadeira rádio on-line, onde ele tocará músicas e apresentará programas discutindo temas da cultura pop atual.

Após o lançamento do site, Leôncio recebe uma cobrança do ECAD, referente aos direitos autorais das músicas tocadas em sua "rádio-site". Em dúvida sobre a legitimidade dessa cobrança, ele procura você para saber se é obrigado ou não a recolher direitos autorais em razão das músicas transmitidas em seu site via *streaming*.

Resolução da situação-problema

A legislação brasileira, especificamente a Lei de Direitos Autorais (Lei nº 9.610/98), não faz qualquer menção direta ao *streaming* de conteúdos protegidos. Como você verificou no *Não pode faltar*, o artigo 68 da Lei de Direitos Autorais determina que não podem ser utilizadas em execução pública ou representação: obras teatrais, composições musicais ou lítero-musicais e fonogramas sem prévia e expressa autorização do autor (BRASIL, 1998, art. 68).

Por sua vez, o termo "execução pública" é definido nesse mesmo artigo como a utilização de composições musicais ou lítero-musicais, mediante a participação de artistas, remunerados ou não, ou a utilização de fonogramas e obras audiovisuais, em locais de frequência coletiva, por quaisquer processos, inclusive a radiodifusão ou transmissão por qualquer modalidade e a exibição cinematográfica.

Resta, então, saber se a cobrança realizada pelo ECAD sobre os direitos autorais das obras transmitidas no site de Leôncio é legítima.

No Recurso Especial nº 1.559.264, a 2ª Seção do Superior Tribunal de Justiça deu provimento ao recurso do ECAD e decidiu que é legítima a arrecadação dos direitos autorais nas transmissões musicais pela internet, via *streaming*.

O ministro Villas Bôas Cueva, relator do processo, destacou que a

transmissão digital via *streaming* pode ser entendida como uma forma de execução pública, tendo em vista que a Lei nº 9.610/98 considera como local de frequência coletiva onde quer que se transmita obras musicais, como seria o caso da internet, sendo irrelevante a quantidade de pessoas que se encontram no ambiente de exibição musical (SERVIÇOS DE STREAMING..., 2017).

Para o ministro, o que caracteriza a execução como pública é o fato de as obras estarem à disposição de uma coletividade frequentadora do ambiente digital, que poderá a qualquer momento acessar o conteúdo ali disponibilizado (SERVIÇOS DE STREAMING...,, 2017).

Dessa maneira, sem adentrarmos no mérito da decisão, é recomendável que Leôncio faça o pagamento dos direitos autorais das músicas tocadas em seu site, de modo a evitar futura condenação judicial.

Faça valer a pena

1. Sobre os nomes de domínio, analise as assertivas a seguir:
I – Será concedido ao primeiro requerente que satisfizer as exigências para registro do nome.
II – É vedada a utilização de expressões que induzam terceiros a erro.
III – É possível o registro para prática de atividades ilícitas.
IV – É possível o uso de palavras abusivas.
Assinale a única alternativa que contém as assertivas corretas.
a) I e II.
b) III e IV.
c) I e IV.
d) II e III.
e) I, II e III.

2. Analise as assertivas a seguir sobre conflitos entre nomes de domínio:
I – Conflito entre nomes de domínio nacionais serão resolvidos apenas pela via judicial.
II – É permitida a solução do conflito pela via arbitral.
III – Os casos que envolvam pedidos de indenização por danos morais ou materiais podem ser resolvidos na via administrativa.
IV – É necessária a demonstração da má-fé no uso de nome de domínio

cujo nome seja marca pertencente a terceiro.
Assinale a única alternativa que contém as assertivas corretas.
a) III e IV.
b) I e IV.
c) I e III.
d) I e II.
e) II e IV.

3. O termo _____ é definido pela Lei de Direitos Autorais como a utilização de composições musicais ou lítero-musicais, mediante a participação de artistas, remunerados ou não, em locais de frequência coletiva, por quaisquer processos. Nesse caso, são cobrados royalties, que ficam a cargo do _____.
Assinale a alternativa que preenche corretamente as lacunas do texto.
a) Execução particular; Escritório Central de Arrecadação e Distribuição (ECAD).
b) Execução pública; Escritório Central de Arrecadação e Distribuição (ECAD).
c) Exibição; Conselho Administrativo de Defesa Econômica (CADE).
d) Representação particular; Poder Judiciário.
e) *Streaming;* Poder Executivo.

Seção 3.3

Contratos e títulos de crédito eletrônicos

Diálogo aberto

Antes de apresentarmos nossa situação-problema, vamos relembrar o contexto de aprendizagem desta unidade? Lembre-se de que você foi contratado por uma empresa startup chamada Piper Comércio Eletrônico, que pretende fornecer a seus usuários uma plataforma que facilita o processo de compra e venda de produtos usados pela internet. Após longo esforço e investimento, o site da empresa encontra-se ativo e operacional. Todavia, alguns problemas, principalmente voltados à devolução de produtos, começaram a ocorrer, em razão de um problema na página do site, que deveria mostrar as especificações técnicas dos produtos oferecidos pelos usuários vendedores. Isso causou confusão entre usuários compradores, sendo que muitos pediram a devolução do dinheiro logo após o recebimento do produto. Nesse caso, a empresa Piper é obrigada a devolver o valor pago pelos usuários compradores, caso decidam exercer seu direito de arrependimento? Ainda, o direito de arrependimento pode ser exercido contra a Piper, ou somente contra o usuário vendedor do produto usado? O mesmo valeria para produtos vendidos por usuários localizados no exterior?

Lembre-se, caro aluno, de que as respostas a esses questionamentos deverão ser expressas na forma de um parecer jurídico.

Não pode faltar

Nesta seção, iremos analisar as questões jurídicas relacionadas ao comércio eletrônico, ou *e-commerce*. O comércio, em seus primórdios, foi desenvolvido através de verdadeiras feiras e bazares, além de caravanas terrestres e marítimas. Atualmente, esses locais onde pessoas circulavam com objetivo de vender produtos e serviços estão sendo, cada vez mais, transpostos para o ambiente eletrônico, sobretudo a internet.

O comércio eletrônico pode ser definido como o conjunto de operações de compra e venda de mercadorias ou prestações de serviços por meio eletrônico ou, em outras palavras, as transações

com conteúdo econômico realizadas por intermédio dos meios digitais (CASTRO, 2002).

Nesse sentido, tanto a oferta quanto a celebração do contrato são realizadas por transmissão e recepção eletrônica de dados e que podem se dar por meio da internet ou fora dela. Todavia, os grandes problemas jurídicos a serem enfrentados se dão, notadamente, no âmbito do comércio eletrônico realizado na rede mundial de computadores.

O comércio eletrônico pressupõe, naturalmente, a contratação à distância entre as partes envolvidas, neste caso, utilizando o meio informático. Daí a importância de estudarmos, primeiramente, as questões relacionadas à contratação eletrônica.

No âmbito brasileiro, os contratos celebrados na internet estão sujeitos aos mesmos princípios e regras aplicáveis aos demais contratos celebrados em território nacional. Portanto, analisaremos alguns dispositivos do Código Civil e do Código de Defesa do Consumidor, tendo em vista a preponderância e a aplicação desses diplomas aos contratos firmados na internet.

Em relação à formação do contrato em ambiente eletrônico, em geral, aplicamos as regras estabelecidas no Código Civil, previstas nos artigos 427 e seguintes, tais como: a manifestação de vontade das partes, oferta, proposta e aceitação.

Que tal relembrar as regras estabelecidas na Seção II do Nosso Código Civil sobre a Formação de Contratos?

Sobre a manifestação de vontade, interessante notar que, tendo em vista a desmaterialização dos instrumentos negociais, notadamente o papel, criaram-se outras alternativas para que as partes manifestassem sua vontade, tais como as assinaturas digitais.

Dentro de um contrato, o consentimento das partes é expresso por meio de sua assinatura. Assinatura é toda marca, sinal ou operação que confira autenticidade à declaração de vontade, fixando seu teor, de forma íntegra no tempo e no espaço, pelo emissor, sendo autenticidade o atributo que atesta a identidade do declarante (a pessoa é quem ela diz ser) e integridade, o atributo que determina que o estado dos dados emitidos pelo declarante não foi alterado após a aposição da assinatura.

Assim, assinar um documento significa também conferir eficácia jurídica e validade a certa declaração de vontade ou a um conjunto de declarações de vontades em um suporte, seja ele digital ou físico, o que estabelece a celebração de um ato jurídico ou contrato entre as partes, respectivamente, nos termos do artigo 104 do Código Civil, senão vejamos:

> **Art. 104. A validade do negócio jurídico requer:**
> **I - agente capaz;**
> **II - objeto lícito, possível, determinado ou determinável;**
> **III - forma prescrita ou não defesa em lei. (BRASIL, 2002, art. 104)**

Então, se for possível identificar a autenticidade da declaração de vontade de todos os envolvidos, tem-se que o negócio jurídico foi perfeitamente constituído e possui plena eficácia no que diz respeito à manifestação de vontade registrada.

Assim, nos termos do artigo 10º da Medida Provisória nº 2.200-2 de 2001, temos que as declarações de vontade ratificadas por assinaturas digitais ou certificados digitais expedidos pela Instituição de Chaves Públicas Brasileiras (ICP-Brasil) são consideradas autênticas em relação a quem as utiliza e não retira a validade de outras formas de assinatura digital, desde que aceitas pelas partes envolvidas ou se forem admitidas de tal forma.

Assimile

Assinar um documento digitalmente significa executar uma função tecnológica que lhe confira uma marca específica e que seja impossível de ser dissociada sem alterar seu conteúdo.

Todos os arquivos digitais possuem alguma espécie de assinatura nativa, por isso os softwares mais recentes já conseguem indicar evidências de autenticidade nos documentos por meio de bytes que não alteram a visualização da tela, mas marcam como o arquivo foi gerado ou até mesmo por quem.

No entanto, esses bytes podem ser alterados se não for executada uma função também tecnológica de controle e bloqueio, a exemplo de metadados ("dados sobre dados") de arquivo que podem ser alterados acionando as propriedades com o botão direito do mouse.

Pesquise mais

Já que estamos falando de **byte** e **bit**, você entende o que significam? Procure ampliar seus conhecimentos:

SIGNIFICADO de Bit e Byte. **Significados**, 2017. Disponível em: <https://www.significados.com.br/bit-e-byte/>. Acesso em: 20 jul. 2017.

São diversas as formas de assinaturas digitais, indo desde uma simples assinatura digitalizada até o uso de biometria ou certificado digital, passando por um simples clique em um *checkbox* onde o usuário eventualmente concorda com os Termos de Uso de um site.

Sobre a oferta e aceitação nos contratos eletrônicos, pode-se dizer que a oferta se dá no momento em que dados disponibilizados no site ingressam no computador do possível adquirente. Já a aceitação acontece quando os dados são efetivamente transmitidos por este às máquinas do titular daquele site.

Os contratos eletrônicos podem ser considerados contratos entre ausentes ou entre presentes, no sentido do disposto no artigo 428 do Código Civil, especialmente em seu inciso I, a depender se a contratação está sendo feita em um sistema com comunicação instantânea ou não. Todavia, tarefa difícil é definir aquilo que é "instantâneo" e aquilo que não é. Vejamos o que diz o aludido artigo:

> **Art. 428. Deixa de ser obrigatória a proposta:**
> **I - se, feita sem prazo a pessoa presente, não foi imediatamente aceita. Considera-se também presente a pessoa que contrata por telefone ou por meio de comunicação semelhante. (BRASIL, 2002, art. 428)**

Exemplificando

Um e-mail, a depender da situação, pode ser considerado uma comunicação instantânea ou não. Se o remetente envia a mensagem, sendo respondido dentro de um curto período de tempo, digamos 60 segundos, a comunicação pode ser considerada instantânea. Mas se tal resposta vier, por exemplo, 24 horas depois do envio, não mais essa comunicação será instantânea.

Independentemente dessa discussão, fato é que nos parece que o sentido do artigo 428, inciso I, do Código Civil, está mais relacionado à questão da "instantaneidade" do que à ausência de contato pessoal das partes. Isso porque entre presentes forma-se o vínculo contratual pela aceitação imediata, ou dentro de um breve prazo. A presença não implica permanência material da pessoa, bastando que as partes troquem suas declarações de modo que a oferta e a aceitação sucedam sem interrupção, como é o caso do telefone, por exemplo (MENDONÇA, 1956).

Ademais, aos contratos eletrônicos são aplicáveis os institutos da teoria geral das obrigações, tais como função social do contrato, boa-fé contratual, além das disciplinas dos contratos de adesão e contratos atípicos.

Então, apresentamos a você os conceitos sobre contratação eletrônica. Vamos abordar, agora, um pouco do comércio eletrônico e a legislação que se aplica. Em relação às normas contidas no Código de Defesa do Consumidor (CDC), temos que, ao comércio eletrônico, elas são plenamente aplicáveis. Nesse sentido, o contrato celebrado na internet entre o usuário e o titular enseja a formação de uma relação de consumo, reconhecendo-se, assim, a vulnerabilidade do usuário, que passará a ter assegurado os direitos básicos do consumidor, tal como a inversão o ônus da prova (BRASIL, 1990, art. 6º).

Entre as práticas comerciais previstas no CDC estão: a oferta, a publicidade (abusiva ou enganosa), a cobrança de dívidas, a proteção das bases de dados, entre outras. Em princípio, qualquer uma dessas práticas pode ocorrer no meio eletrônico, o que atrai a aplicação da legislação específica.

No que tange à proteção contratual, resta estabelecido no CDC o princípio da interpretação mais favorável aos consumidores, as declarações de vontade, o direito de arrependimento, cláusulas abusivas, etc. Já na questão dos bancos de dados e cadastros dos consumidores, por exemplo, o artigo 43 do CDC prevê que os consumidores têm pleno acesso às informações neles contidas, aplicando-se ainda os princípios de proteção de dados pessoais estudados na Unidade 2.

Ademais, o CDC trata especificamente do comércio eletrônico por meio do Decreto nº 7.962 de 2013. Tal decreto tem por escopo

promover a disponibilização de informações pelos fornecedores sobre si próprios, seus produtos e serviços, além de garantir um atendimento facilitado ao consumidor e o respeito ao direito de arrependimento.

Sobre o direito de arrependimento, cumpre salientar que houvesse quem defendesse sua não aplicação às compras feitas pela internet. Isto porque o artigo 49 do CDC fazia referência às compras feitas fora do estabelecimento do fornecedor, sendo que o "estabelecimento" seria formado pelo conjunto de bens corpóreos e incorpóreos, de titularidade da pessoa jurídica, incluindo nesta última categoria o website de titularidade do fornecedor. Todavia, com o advento do referido decreto tal teoria foi descartada, nos termos do artigo 5º do citado diploma:

> Art. 5º O fornecedor deve informar, de forma clara e ostensiva, os meios adequados e eficazes para o exercício do direito de arrependimento pelo consumidor.
> § 1º O consumidor poderá exercer seu direito de arrependimento pela mesma ferramenta utilizada para a contratação, sem prejuízo de outros meios disponibilizados.
> § 2º O exercício do direito de arrependimento implica a rescisão dos contratos acessórios, sem qualquer ônus para o consumidor.
> § 3º O exercício do direito de arrependimento será comunicado imediatamente pelo fornecedor à instituição financeira ou à administradora do cartão de crédito ou similar, para que:
> I - a transação não seja lançada na fatura do consumidor; ou
> II - seja efetivado o estorno do valor, caso o lançamento na fatura já tenha sido realizado. (BRASIL, 2013, art. 5º)

Ainda sobre o direito de arrependimento, o artigo 5º do decreto acima transcrito dispõe que o fornecedor deve informar, de forma clara e ostensiva, os meios adequados e eficazes para o consumidor exercer o direito de arrepender-se. O fornecedor deverá enviar ao consumidor confirmação imediata do recebimento da manifestação de arrependimento, sendo que o exercício do direito implica na rescisão dos contratos acessórios (ex.: cartão de crédito), sem qualquer ônus ao consumidor.

Reflita

Caso o Decreto n. 7.962 de 2013 fosse silente em relação à aplicabilidade do direito de arrependimento às compras feitas on-line, na sua opinião, tal direito seria realmente aplicável em compras dessa natureza? Para responder esse questionamento, leve em consideração o conceito de "estabelecimento comercial" à própria natureza jurídica desse instituto, que foi criado com objetivo de proteger o consumidor de ofertas agressivas.

Entre suas inovações, o Decreto 7.963 de 2013, em seu art. 2º, determinou que, para realizar a conclusão de contrato, os sites devem disponibilizar, em local de destaque, o: nome empresarial; o número de cadastro do fornecedor no CPF ou no CNPJ; endereço físico e eletrônico; além de outras informações pertinentes a sua localização e contato. Vejamos:

> Art. 2º Os sítios eletrônicos ou demais meios eletrônicos utilizados para oferta ou conclusão de contrato de consumo devem disponibilizar, em local de destaque e de fácil visualização, as seguintes informações:
> I - nome empresarial e número de inscrição do fornecedor, quando houver, no Cadastro Nacional de Pessoas Físicas ou no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda;
> II - endereço físico e eletrônico, e demais informações necessárias para sua localização e contato;
> III - características essenciais do produto ou do serviço, incluídos os riscos à saúde e à segurança dos consumidores;
> IV - discriminação, no preço, de quaisquer despesas adicionais ou acessórias, tais como as de entrega ou seguros;
> V - condições integrais da oferta, incluídas modalidades de pagamento, disponibilidade, forma e prazo da execução do serviço ou da entrega ou disponibilização do produto; e
> VI - informações claras e ostensivas a respeito de quaisquer restrições à fruição da oferta. (BRASIL, 2013, art. 2º)

Além disso, devem estar presentes na oferta (eletrônica) do produto ou serviço suas características essenciais, inclusive acerca de riscos à saúde e segurança do consumidor, a discriminação, no preço, de eventuais despesas adicionais ou acessórias, como entrega e seguros, além de formas de pagamento, disponibilidade, entre outras.

Interessante notar que o decreto trouxe também regras para os fornecedores de sites de compras coletivas. Conforme seu artigo 3º, os sites dessa categoria de comércio ou assemelhados deverão conter, quando for o caso, a quantidade mínima de consumidores para a efetivação do contrato; o prazo para utilização da oferta pelo consumidor; a identificação do fornecedor responsável pelo site e do fornecedor do produto ou serviço ofertado. Confira-se:

> **Art. 3º Os sítios eletrônicos ou demais meios eletrônicos utilizados para ofertas de compras coletivas ou modalidades análogas de contratação deverão conter, além das informações previstas no art. 2º, as seguintes:**
> **I - quantidade mínima de consumidores para a efetivação do contrato;**
> **II - prazo para utilização da oferta pelo consumidor; e**
> **III - identificação do fornecedor responsável pelo sítio eletrônico e do fornecedor do produto ou serviço ofertado, nos termos dos incisos I e II do art. 2º. (BRASIL, 2013, art. 3º)**

Resumidamente, o decreto veio para reafirmar o que já é pacífico na doutrina e na jurisprudência sobre a admissibilidade da aplicação do CDC às relações de consumo estabelecidas no meio eletrônico. Percebe-se que muitas de suas disposições já estão disciplinadas no próprio CDC, como o direito do consumidor às informações claras sobre produtos e serviços.

Pesquise mais

Atualmente, encontra-se em tramitação o Projeto de Lei nº 281 de 2012. Esse projeto de lei tem por objetivo consolidar algumas das regras já previstas no Decreto nº 7.962, bem como ampliar alguns direitos básicos do consumidor, levando em consideração o estado atual da economia digital. Entre as alterações, citamos as normas referentes à proteção de dados pessoais dos consumidores eletrônicos e a possibilidade de dilação do prazo para exercício do direito de arrependimento, que poderá ser de 14 dias, caso o fornecedor não facilite o exercício desse direito por meio de envio de formulários específicos. Que tal pesquisar um pouco mais sobre esse assunto?

Mas como ficam as relações estabelecidas entre consumidores brasileiros e sites de comércio eletrônico internacionais?

Em que pese o artigo 3º do CDC abarcar no conceito de "fornecedor" as pessoas físicas ou jurídicas sediadas no exterior, temos que, na prática, conseguir dar efetividade a uma ação judicial nesses termos é algo extremamente complexo, haja vista a dificuldade em citar a pessoa estrangeira e obter executividade de eventual sentença favorável.

Uma possível solução a esses problemas, que porém não é unânime na doutrina, é recorrer às regras do Direito Internacional Privado, em especial às disposições do **Decreto-Lei nº 4.657, de 4 de setembro de 1942** – Lei de Introdução às Normas de Direito Brasileiro (LINDB).

O art. 9º dispõe que se aplicará a lei do país em que as obrigações (contratos) se constituíram. Uma vez que a internet é um ambiente sem fronteiras, fica difícil afirmar em qual país um contrato eletrônico, firmado por partes sediadas em países diversos, foi constituído. Entretanto, o §2º desse mesmo art. 9º estabelece que, na obrigação decorrente de contrato, considera-se este constituído no lugar em que residir o proponente, nesse caso o titular do website onde a compra foi realizada.

Por outro lado, há quem afirme ser inaplicáveis as normas da LINDB, tendo em vista ser essa norma mais específica. Além disso, resta consagrada a "lei de residência do consumidor", nos termos do Protocolo de Santa Maria sobre jurisdição internacional em matéria de relações de consumo, entre outros diplomas internacionais (CRUZ, 2006).

Reflita

Na sua opinião, as normas da LINDB seriam aplicáveis aos contratos internacionais? Ou o consumidor permanece amparado pelo CDC?

Continuando nossos estudos acerca do comércio eletrônico, vamos falar um pouco sobre a informática e os títulos de crédito, passando para a etapa final, que se relaciona juntamente a uma das etapas finais de um compra, o pagamento. A maneira mais comum dos usuários realizarem o pagamento das compras realizadas no meio eletrônico é, certamente, por meio dos cartões de crédito e débito. Daí a necessidade de estudarmos alguns aspectos relacionados aos títulos de crédito eletrônicos.

Primeiramente, iremos investigar a natureza jurídica do cartão de crédito e do cartão de débito, com objetivo de sabermos se eles podem ser tidos como uma ordem de pagamento e, consequentemente, uma evolução do conhecido cheque, ou se são meros substitutos dele.

Especificamente em relação ao cartão de débito, trata-se de uma operação contratual entre banco e cliente em que aquele se compromete a efetuar débitos na conta bancária deste, mediante ordem de pagamento, feita pelo meio eletrônico. É verdadeira autorização de débito. Nesse sentido, o cartão de débito pode ser visto como uma espécie de "cheque eletrônico" (TEIXEIRA, 2015).

Reflita

Você acredita que, nesses tempos de aumento de compras eletrônicas pela internet, o cartão de crédito é a forma de pagamento mais segura? Será que existem outras formas de pagamento em que o comprador fique menos exposto a determinados riscos, tal como a clonagem de seu cartão?

Por outro lado, entendemos que o cartão de crédito se trata de instrumento jurídico diverso do cheque. Isso porque sua natureza jurídica não pode ser considerada como a de um título de crédito. Sua estrutura envolve um sistema, formado por diferentes contratos que interagem entre si, constituindo um corpo próprio, com características típicas e peculiares, tendo como natureza jurídica um contrato plurilateral, atípico, de crédito, de adesão, de consumo e comutativo (AVELAR, 2014).

Pesquise mais

Para saber mais sobre a natureza jurídica do cartão de crédito, sugerimos a leitura do artigo a seguir:

MIRANDA, Maria Bernadete. Aspectos Jurídicos do Contrato de Cartão de Crédito. **Revista Virtual Direito Brasil**, v. 4, n. 1, 2010. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/aspectos_juridicos_do_contrato_de_cartao_de_credito.pdf>. Acesso em: 11 jul. 2017.

Em conclusão, vimos que o comércio eletrônico é uma evolução natural do "comércio de rua", que se utiliza das vias digitais para sua realização. Igualmente, diversos institutos jurídicos convergem para regular essa atividade, com destaque para o próprio Código Civil e o Código de Defesa do Consumidor.

Sem medo de errar

Antes de resolvermos nossa situação-problema, vamos retomá-la?

O site da nossa cliente, a empresa Piper, apresentou problema na página que deveria mostrar as especificações técnicas dos produtos oferecidos pelos usuários vendedores. Isso causou confusão entre usuários compradores, sendo que muitos pediram a devolução do dinheiro logo após o recebimento do produto. Nesse caso, a empresa Piper é obrigada a devolver o valor pago pelos usuários compradores, caso eles decidam exercer seu direito de arrependimento? Ainda, o direito de arrependimento pode ser exercido contra a Piper, ou somente contra o usuário vendedor do produto usado? O mesmo valeria para produtos vendidos por usuários localizados no exterior? Lembre-se de que as respostas a esses questionamentos deverão ser expressas na forma de um parecer jurídico.

APLICABILIDADE DO DIREITO DE ARREPENDIMENTO AO COMÉRCIO ELETRÔNICO

Em que pese a empresa Piper não ser a vendedora do produto usado, ela forneceu toda a infraestrutura tecnológica utilizada para a realização da operação, sendo que, nesse caso, ao auferir lucros com atividades dos usuários, ela se enquadra no conceito de "fornecedor", nos termos do CDC.

Verificada a relação de consumo, temos que o comércio eletrônico é regulado, de maneira específica, pelo Decreto nº 7.962 de 2013. Referido diploma legal dispõe que os usuários do site têm direito às informações claras sobre os produtos comprados. Tendo em vista que o problema acerca das informações sobre os produtos vendidos originou-se do próprio site da empresa, verificamos aí uma violação da norma consumerista, além de vício no serviço prestado pelo site.

Mas, independentemente da presença de vícios no produto ou nos serviços oferecidos pelo site, fato é que o referido decreto veio acabar com as discussões acerca da aplicabilidade do direito de arrependimento para as compras on-line.

Assim, os usuários do site têm direito de se arrependerem da compra, sendo a empresa Piper obrigada a devolver o valor da compra, sem qualquer ônus ao consumidor/usuário.

No caso do usuário vendedor estar localizado no exterior, em nada prejudicaria o usuário comprador, eis que o direito de arrependimento, como dito anteriormente, poderá ser exercido tanto em face da Piper quanto do usuário vendedor.

Avançando na prática

Compras coletivas na internet

Descrição da situação-problema

A empresa Coshopping, que se dedica à oferta de compras coletivas por meio de seu site, está sendo processada, em litisconsorte passivo, por vários usuários que compraram um *voucher* de uma empresa que anunciava em seu site a compra coletiva de produtos alimentícios, especificamente vinhos importados.

Nos termos da promoção, os usuários se juntariam para comprar um lote de vinhos importados com 50% (cinquenta por cento) de desconto sobre o valor original. Ocorre que a empresa que realizou o anúncio jamais entregou os produtos adquiridos pelos usuários compradores, alegando que não foi atingido o número mínimo de compradores. Igualmente, a empresa se recusou a devolver o dinheiro. Você, como julgador da causa, condenaria a empresa Coshopping, de maneira solidária à empresa anunciante, pelos danos sofridos pelos usuários?

Para responder essa questão, considere que no anúncio da compra coletiva não constavam nem as informações completas acerca do anunciante, nem a quantidade mínima de usuários necessária para entrega das mercadorias.

Resolução da situação-problema

Para resolvermos essa questão, temos que, novamente, nos socorrer das normas contidas no Decreto nº 7.962 de 2013. Conforme seu artigo 3º, os sites de compras coletivas ou assemelhados, como é o caso da empresa Coshopping, deverão constar, em seus anúncios, quando for o caso, a quantidade mínima de consumidores para a efetivação do contrato; o prazo para utilização da oferta pelo consumidor; a identificação do fornecedor responsável pelo site e do fornecedor do produto ou serviço ofertado. Uma vez que o site

não apresentava tais informações, verifica-se a ocorrência de vício no serviço prestado pelo site de compra coletiva, que não estava em conformidade legal. Assim, deverá responder de maneira solidária pelos danos causados aos usuários compradores.

Faça valer a pena

1. Até mesmo os contratos eletrônicos exigem como requisito a manifestação de vontade das partes expressa, implicando na aceitação das cláusulas contratuais. Por serem contratos prontos, nos chamados "contratos de adesão" não há a discussão das cláusulas.
Assinale a alternativa que corretamente indica como pode se dar a aceitação do contrato, no caso dos contratos eletrônicos.
a) Não é necessária concordância expressa.
b) Basta o download dos arquivos, sem concordância expressa.
c) O aceite do contrato pode se dar automaticamente.
d) Por meio de assinatura digital.
e) Negativa ao termo de aceite.

2. Quanto aos usuários do comércio eletrônico, é aplicável o _____, como instrumento de proteção dos consumidores. Um dos direitos básicos contidos em tal legislação é o do(a) _____, pois o consumidor é considerado parte hipossuficiente na relação, inclusive em juízo.
Assinale a única alternativa que completa corretamente as lacunas do texto.
a) Código de Defesa do Consumidor; ônus da prova exclusivo do consumidor.
b) Código Penal; direito de arrependimento.
c) Código de Processo Penal; inversão do ônus da prova.
d) Código de Processo Civil; direito ao contraditório.
e) Código de Defesa do Consumidor; direito de arrependimento.

3. Sobre os contratos eletrônicos, analise as afirmações a seguir, fazendo a correta associação entre as colunas:
( ) Oferta.
( ) Aceitação.
( ) Assinatura digital.
A. Se dá no momento em que dados disponibilizados no site ingressam no computador do possível adquirente.
B. Método de autenticação de informações digitais.
C. Ocorre quando os dados são transmitidos do adquirente ao titular do site.
Assinale a única alternativa que contém a associação correta entre os conceitos.
a) (A), (C), (B).
b) (A), (B), (C).
c) (C), (B), (A).
d) (B), (C), (A).
e) (B), (A), (C).

Referências

AVELAR, Daniel Duarte Costa de. As peculiaridades do contrato de cartão de crédito. **Jus**, dez. 2014. Disponível em: <https://jus.com.br/artigos/34862/as-peculiaridades-do-contrato-de-cartao-de-credito>. Acesso em: 23 jul. 2017.

BAEZ, Narciso Leandro Xavier; RESCHKE, Ana Paula Goldani Martinotto. A evolução histórica da propriedade até o Estado Liberal. In: ANDREUCCI, Álvaro G. A.; MAGALHÃES, Juliana N.; SIQUEIRA, Gustavo S. (Coord.). **História do direito** [Recurso eletrônico online]. Florianópolis: Conpedi, 2015. p. 383-389. Disponível em: <https://www.conpedi.org.br/publicacoes/66fsl345/gv4u3hv2/Tltbuh539SSiT0be.pdf>. Acesso em: 16 jul. 2017.

BARBOSA, Denis Borges. **O conceito de propriedade intelectual**. 2002. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/27573-27583-1-PB.pdf>. Acesso em: 16 jul. 2017.

_____. **Nota sobre a noção de segredo de empresa**. 2008. Disponível em: <http://denisbarbosa.addr.com/arquivos/200/propriedade/nota_segredo.pdf>. Acesso em: 16 jul. 2017.

BIG Data e Internet das Coisas serão motores de uma nova economia. **Computerworld,** 17 jun. 2015. Disponível em: <http://computerworld.com.br/big-data-e-internet-das-coisas-serao-motores-de-uma-nova-economia>. Acesso em: 5 jul. 2017.

BITTAR, Carlos Alberto. **Direito de autor**. 3. ed. Rio de Janeiro: Forense Universitária, 2000.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 5 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 7 ago. 2017.

_____. Lei nº 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. **Diário Oficial da União**, Brasília, 15 maio 1996.

_____. Lei nº 9.610, de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. **Diário Oficial da União**, Brasília, 20 fev. 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9610.htm>. Acesso em: 13 ago. 2017.

_____. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, 11 jan. 2002.

_____. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União,** Brasília, 12 set. 1990.

_____. Decreto nº 7.962, de 15 de março de 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. **Diário Oficial da União**, Brasília, 15 mar. 2013.

CASTRO, Aldemário Araújo. Os meios eletrônicos e a tributação. In: REINALDO FILHO, Demócrito (Coord.). **Direito de Informática**: temas polêmicos. Bauru: Edipro, 2002.

CRETELLA JÚNIOR, José. **Curso de Direito Romano**. 19. ed. Rio de Janeiro: Forense, 1995.

CRUZ, Carolina Dias Tavares Guerreiro. **Contratos internacionais de consumo**: lei aplicável. Rio de Janeiro: Forense, 2006.

GRADO, Milena Mendes. A legalidade do pagamento de direitos autorais relativos à execução pública sobre o *streaming*. **Patrícia Peck Pinheiro**, [2014a]. Disponível em: <http://pppadvogados.com.br/publicacoes/a-legalidade-do-pagamento-de-direitos-autorais-relativos-a-execucao-publica-sobre-o-streaming>. Acesso em: 4 jul. 2017.

HAMANN, Renan. 5 segredos industriais guardados a sete chaves. **Tecmundo,** 31 jan. 2012. Disponível em: <https://www.tecmundo.com.br/curiosidade/18707-5-segredos-industriais-guardados-a-sete-chaves.htm>. Acesso em: 16 jul. 2017.

MENDONÇA, Manuel Inácio Carvalho de. **Doutrina e prática das obrigações.** 4. ed. aum. e atual. por José de Aguiar Dias. Rio de Janeiro: Forense, 1956. v. 2.

MIRANDA, Maria Bernadete. Aspectos Jurídicos do Contrato de Cartão de Crédito. **Revista Virtual Direito Brasil**, v. 4, n. 1, 2010. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/aspectos_juridicos_do_contrato_de_cartao_de_credito.pdf>. Acesso em: 11 jul. 2017.

MONTEIRO, Washington de Barros. **Curso de direito civil: direito das coisas**. 34. ed. atual. São Paulo: Saraiva, 1998. v. 3.

PINHEIRO, Patrícia Peck. **Direito digital**. São Paulo: Saraiva, 2015.

ROHRMANN, Carlos Alberto. **Estudos e pesquisas em direito empresarial na contemporaneidade**: propriedade intelectual e tecnologia. Belo Horizonte: RTM, 2015.

SERVIÇOS de streaming de músicas deverão pagar direitos autorais ao Ecad. STJ, 10 ago. 2017. Disponível em: <http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunica%C3%A7%C3%A3o/noticias/Not%C3%ADcias/Servi%C3%A7os-de-streaming-de-m%C3%BAsicas-dever%C3%A3o-pagar-direitos-autorais-ao-Ecad>. Acesso em: 13 ago. 2017.

SIGNIFICADO de Bit e Byte. **Significados**, 2017. Disponível em: <https://www.significados.com.br/bit-e-byte/>. Acesso em: 20 jul. 2017.

TEIXEIRA, Tarcísio. **Curso de direito e processo eletrônico**: doutrina, jurisprudência e prática. 3. ed. atual. e ampl. São Paulo: Saraiva, 2015.

TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. **Registro de domínio semelhante na internet é concorrência desleal**. Disponível em: <https://tj-rs.jusbrasil.com.br/noticias/647353/registro-de-dominio-semelhante-na-internet-e-concorrencia-desleal>. Acesso em: 21 ago. 2017.

Delitos informáticos

Convite ao estudo

O uso da internet para prática de crimes tornou-se algo comum em nosso cotidiano. Somente no passado recente é que as primeiras leis específicas sobre o tema foram aprovadas no Brasil. Dessa maneira, não existe uma jurisprudência consolidada sobre o tema, o que gera muita insegurança, tanto por parte dos usuários, quanto por parte de empresas e profissionais de TI. Na unidade anterior, estudamos a proteção dos bens intangíveis, dotados de valor econômico, por alguns institutos jurídicos, como a propriedade intelectual. Nesta unidade, nosso foco será a proteção dos usuários sob o ponto de vista do Direito Penal, ou seja, iremos estudar as diversas facetas dos delitos informáticos.

Para tanto, caro aluno, iremos considerar o seguinte contexto de aprendizagem: você, na condição de advogado, foi procurado por uma família com o objetivo de orientá-los sobre um recente caso envolvendo a filha mais nova do casal. Essa filha, que na data da consulta tinha 14 anos, teve fotos íntimas divulgadas na internet, sendo tal conteúdo posteriormente vinculado em um site de pornografia infantil. A família não sabe ao certo como tais fotos foram parar na internet, tendo em vista que a filha mais nova as tirava em âmbito privado, na sua própria casa, e depois as "carregava" em seu computador pessoal. A menor afirma que jamais enviou tais conteúdos para qualquer pessoa. Tendo em vista tal situação, você deverá elaborar uma queixa-crime em desfavor do potencial criminoso que invadiu o dispositivo da jovem. Para tanto você deverá considerar as seguintes indagações: É possível verificar se houve eventual invasão ao dispositivo informático da filha mais nova? Tal conduta ("invadir dispositivo informático") é punível em nossa legislação? A partir da resposta a tais questionamentos, você deverá elaborar uma queixa-crime para posterior atuação do Ministério Público.

Para resolver as situações-problemas derivadas do contexto de aprendizagem descrito, iremos estudar na Seção 4.1 a evolução histórica dos crimes eletrônicos, sua classificação doutrinária, sua contextualização em âmbito global, as dificuldades e resoluções encontradas pelo legislador brasileiro para tentar combater a criminalidade informática.

Na Seção 4.2 iremos aprofundar o conteúdo, analisando como se dá o enquadramento legal das principais condutas ilícitas praticadas no meio eletrônico, analisando ainda, com mais detalhes, a preocupante exposição das crianças e dos adolescentes na internet.

Por fim, na Seção 4.3, iremos estudar mais detidamente os casos análogos aos previsto na Lei nº 12.737/2012 e a obtenção de provas eletrônicas por meio de técnicas de forense computacional.

Seção 4.1

Meio eletrônico e delitos

Diálogo aberto

Caro aluno, após analisarmos nosso contexto de aprendizagem, iremos passar para nossa situação-problema, que trata, substancialmente, de um problema típico do cotidiano do combate aos delitos informáticos, que diz respeito justamente à questão da territorialidade, ou local do crime, que você deve ter estudado no seu curso de Direito Penal.

Retomando o nosso contexto, você, como advogado, teria de orientar uma família sobre um recente envolvimento da filha mais nova em divulgação de fotos íntimas na internet, sendo que o conteúdo foi vinculado em um site de pornografia infantil.

Após perícia realizada no computador da jovem, descobriu-se que o número IP utilizado para invadir o dispositivo está vinculado a um provedor de conexão localizado na Argentina. Munido de tal informação, você enviou uma notificação extrajudicial ao provedor, inteirando-o da situação e requerendo os dados do titular daquele IP, o que foi prontamente atendido, tendo em vista a política de combate à pornografia infantil da empresa. Descobriu-se que o criminoso é brasileiro, mas que estava utilizando uma ferramenta de conexão privada (VPN) para mascarar o real local de sua conexão. Nesse caso, qual o juízo competente para se propor a queixa-crime? O brasileiro ou o argentino? Lembre-se de que esta deverá ser a primeira parte de sua queixa-crime, seu produto final.

Para resolver essa e outras questões, iremos estudar nesta seção a evolução histórica dos crimes eletrônicos, sua classificação doutrinária, sua contextualização em âmbito global, as dificuldades e resoluções encontradas pelo legislador brasileiro para tentar combater a criminalidade informática.

Não pode faltar

Ao longo dos nossos estudos, constatamos que a Sociedade da Informação possui diversas características peculiares, pautadas principalmente pelas novas tecnologias da informação. Igualmente, estudamos os benefícios que essas tecnologias trazem para os usuários e cidadãos. Entretanto, o mundo digital possui um lado obscuro. Trata-se da criminalidade digital.

Os usuários dessas tecnologias, notadamente os menos informados ou inexperientes, constituem presa fácil nas mãos dos especialistas em crimes cibernéticos, os chamados *crackers*.

Assimile

De uma forma geral, **hackers** são indivíduos que elaboram e modificam softwares e hardwares de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas. Já ***cracker*** é o termo utilizado para designar quem pratica a quebra (ou *cracking*) de um sistema de segurança. Na prática, os dois termos servem para conotar pessoas que têm habilidades com computadores; porém, cada um dos "grupos" usa essas habilidades de formas diferentes. Os hackers usam seu conhecimento para melhorar softwares de forma legal, buscando vulnerabilidades, mas nunca invadem um sistema com o intuito de causar danos. Por outro lado, os *crackers* têm como prática a quebra da segurança de um sistema, usando seu conhecimento de forma ilegal, com objetivo de causar danos a pessoas e empresas.

A tecnologia concede um grande poder a programadores, profissionais de segurança, e outros que conheçam a fundo suas particularidades. Ocorre que o mau uso desse poder para finalidades escusas ou ilícitas torna-se um risco considerável, principalmente em um país onde a educação digital é praticamente ignorada.

Assim, faz-se necessário um mínimo de controle para fazer frente àqueles que cometem condutas antissociais contra os bens informáticos ou por meio deles. Tal controle, ao nosso entendimento, deve ser realizado pelo Estado, através de seus órgãos jurisdicionais. Daí a ciência jurídica necessitar se manter atualizada com as novas formas de criminalidade digital.

Leis que estabeleçam os direitos de usuários na internet e deveres dos prestadores de serviços são fundamentais para que o Judiciário

possa fazer frente a violações e riscos inerentes à sociedade da informação, e, sobretudo, de modo a evitar decisões contraditórias e injustiças face aos casos concretos. Dessa maneira, regulações de natureza civil são primordiais para definir esses direitos e limites dos usuários.

No entanto, o Brasil seguiu por um caminho não muito ortodoxo. Nosso legislador preferiu, primeiramente, adotar a legislação criminal, que deveria ser considerada última opção, para punir condutas praticadas por intermédio ou contra sistemas informáticos.

Após 15 anos de discussões, foram promulgadas as Leis nº 12.735/2012 e nº 12.737/2012, que passaram a fazer frente a algumas condutas ilícitas na seara informática, para prever e combater crimes eletrônicos de maneira efetiva, seja inovando a legislação penal ou ampliando os recursos dos órgãos investigativos. Os direitos dos usuários vieram somente depois, no ano de 2014, com o Marco Civil da Internet, o qual já estudamos. Tal caminho é, no mínimo, temerário, pois uma sociedade que não está preparada para entender o que pode caracterizar ou não um crime informático arrisca violar os direitos de seus usuários, tipificando certas condutas de maneira inconsequente.

Não estamos aqui a condenar a iniciativa do legislador em criar tipos legais com objetivo de punir crimes informáticos. A iniciativa é louvável e serve para acabar com o sentimento de impunidade que paira sobre esse meio. Sabemos que, pelo princípio da legalidade, não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Isso significa que o uso de analogias no campo do Direito Penal é algo vedado. Assim, a inexistência de tipos legais específicos possui a capacidade de suprir eventuais lacunas legislativas.

Entretanto, o processo legislativo deve ser conduzido com cuidado, de modo a evitar pontos obscuros e omissos nas normas penais criadas. Como citamos anteriormente, o Brasil optou por adotar normas penais antes de garantir direitos dos usuários. Infelizmente, o processo de votação das Leis nº 12.735/2012 e nº 12.737/2012 não foi pautado por discussões e reflexões sobre o tema. Pelo contrário, sua aprovação se deu em meio ao furor midiático, em incidente envolvendo uma atriz de uma das maiores emissoras de TV do nosso país.

Pesquise mais

A Lei nº 12.737/2012, mesmo antes de sua aprovação, recebeu o nome de "Lei Carolina Dieckmann". Tal apelido se deu em razão da repercussão do caso no qual *crackers* do interior de Minas Gerais e São Paulo invadiram o e-mail da atriz Carolina Dieckmann, de onde baixaram diversas fotos íntimas da atriz. O conteúdo foi publicado na internet após a atriz resistir às chantagens dos criminosos, que pediram R$ 10.000,00 para apagar as imagens. O caso da atriz serviu de combustível para agilizar a aprovação da cotada lei. Procure se inteirar um pouco mais sobre os detalhes em:

VALLE, J. D. Lei Carolina Dieckmann entra em vigor nesta terça-feira. **Veja**, 2 abr. 2013. Disponível em <http://veja.abril.com.br/tecnologia/lei-carolina-dieckmann-entra-em-vigor-nesta-terca-feira/>. Acesso em: 8 ago. 2017.

Fato é que sempre foi um grande desafio tratar de crimes informáticos com um Código Penal que data da década de 1940. Referido diploma legal é omisso em questões onde a informática deveria ser o bem protegido pelo Direito Penal.

Não se tratava a informática como um bem jurídico relevante, merecedor da tutela do Direito Penal. O desenvolvimento da tecnologia levou a uma sociedade altamente dependente da informática, sendo que a partir desse momento o Direito passou a reconhecer outros valores penalmente relevantes. Diante da evolução tecnológica, existe uma predisposição social em reconhecer bens jurídicos informáticos e, entre os que mais se sobressaem, temos o sigilo e a segurança de dados e informações eletrônicas.

Elevaram-se, pois, os dados informáticos e os dispositivos ao status de valores jurídicos fundamentais das relações sociais de uma sociedade dependente da tecnologia da informação, protegendo-os. Assim, ao tratarmos de "crimes informáticos" ou "delitos informáticos", usamos tal nomenclatura justamente para demonstrar qual o bem jurídico protegido pelo Direito Penal, a informática, ou a privacidade e a integridade dos dados informáticos.

Os crimes ou delitos informáticos podem ser entendidos como fenômenos inerentes às transformações tecnológicas que a sociedade experimenta e que influenciam diretamente no Direito Penal.

Assimile

Conceituamos crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação (JESUS, 2016, p. 49). Nesse sentido, a informática ou é o bem ofendido ou o meio para ofensa a bens já protegidos pelo Direito Penal.

A maior parte dos crimes eletrônicos está relacionada a delitos em que o meio para a realização da conduta é virtual, mas o crime em si não. A exemplo, tem-se como crimes mais comuns praticados na rede o estelionato (fraude) e a pornografia infantil. Já os ataques mais comuns são aqueles praticados por meio de vírus de computador. Assim, em que pese o Direito Penal já proteger certos bens jurídicos agredidos por meio de recursos informáticos, os dados e a segurança dos sistemas clamavam por proteção jurídica específica.

Levando em consideração o bem jurídico ofendido, podemos classificar os delitos informáticos em: delitos informáticos próprios; delitos informáticos impróprios; delitos informáticos mistos; delitos informáticos mediatos ou indiretos (JESUS, 2016, p. 52).

Os "delitos informáticos próprios" são aqueles em que o bem jurídico ofendido é a tecnologia da informação em si. Para esses delitos, a legislação penal era lacunosa, sendo que, diante da vedação às analogias no Direito Penal, muitas práticas não poderiam ser enquadradas criminalmente.

Os "delitos informáticos impróprios" são aqueles em que a tecnologia da informação é o meio utilizado para a agressão a bens jurídicos já tutelados pelo Código Penal. Para esses delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais.

Já os "delitos informáticos mistos" são os crimes complexos em que, além da proteção do bem jurídico informático, a legislação protege outro bem jurídico. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico.

Por último, os "delitos informáticos mediatos (ou indiretos)" são aqueles delitos informáticos praticados para a ocorrência de um delito não informático consumado ao final. No Direito Eletrônico, comumente um delito informático é cometido como meio para a prática de um delito-fim de ordem patrimonial.

Exemplificando

Um exemplo de "delitos informáticos mediatos (ou indiretos)" pode ser o caso do agente que captura dados bancários e usa para desfalcar a conta-corrente da vítima. Pelo princípio da consunção, o agente só será punido pelo delito-fim (furto).

Uma questão polêmica quando o assunto é crime informático refere-se à competência e ao lugar do crime. Nesse sentido, a territorialidade encontra guarida nos Códigos Penal e de Processo Penal. Determinar a territorialidade implica determinar o juiz competente para processar e julgar um delito informático. Pontua-se que o Direito Penal brasileiro está associado ao território nacional, e o que se procede fora de tais limites resulta em revisão de acordos entre os países.

No que tange ao local do crime, o Código Penal adotou, em seu art. 6º, a teoria da ubiquidade, sendo considerado o lugar do crime o local onde ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria se produzir o resultado. Dessa maneira, ao se considerar alguém no estado de Minas Gerais que invade o computador de outrem, localizado no estado do Acre, teríamos o juízo onde está o dispositivo invadido como competente para processar e julgar o delito informático.

No que diz respeito a condutas ilícitas praticadas em território estrangeiro, não se aplicariam as normas brasileiras, considerando a soberania do país, sendo que a questão deverá ser tratada pela extradição. Logicamente que a autoridade brasileira é competente para processar um crime digital praticado por agente brasileiro no exterior, com vítima no Brasil, mas dependerá que esse agente adentre o território brasileiro.

Ademais, nos termos do §2º do art. 70 do Código de Processo Penal, quando atos executórios tenham ocorrido fora do Brasil, a competência será do local onde a infração se deu ou foi concluída a ação delituosa (resultado).

Quanto às investigações formais desses crimes, temos que alguns estados brasileiros têm criado delegacias de polícia especializadas em crimes informáticos. Por exemplo, pode-se citar a Polícia Civil de São Paulo, que já possui Delegacia Especializada desde 2001, e

que investiga crimes de informática próprios e impróprios, atuando somente naqueles crimes praticados na cidade de São Paulo, sendo que tal competência se estabelece pelo domicílio da vítima.

A existência de órgãos investigativos específicos e qualificados é fundamental para identificação dos autores de crimes informáticos. Isso porque a internet, por ser um ambiente virtual de dimensões incalculáveis, proporciona várias formas de cometimento desse tipo de crime. Entre esses meios, destacamos aqueles que consideramos os principais, em razão do número de vítimas: a) vírus – são programas escritos em linguagem de programação que fazem a contaminação de outros programas de computador, por meio de sua modificação, de forma a incluir uma cópia de si mesmo; b) *trojans* – chamados de Cavalos de Troia ou *backdoors*, consistem em programas enviados a um sistema anfitrião, permitindo a conexão do computador infectado com o computador do invasor, sem a necessidade de qualquer autorização. Assim, o remetente controla e monitora grande parte das atividades do usuário hospedeiro; c) *worms* – são programas que se propagam de um sistema para outro, automaticamente, por meio de autoprodução, sem interferência do usuário infectado.

Pesquise mais

Recentemente, temos testemunhado um crescimento exponencial nos ataques do tipo *ransomware*. O *ransomware* (também conhecido como *rogueware* ou *scareware*) restringe o acesso ao sistema de um computador e pede o pagamento de um resgate para que a restrição seja removida. Os ataques de *ransomware* mais perigosos são causados pelos códigos maliciosos WannaCry, Petya, Cerber, Cryptolocker e Locky. Pesquise um pouco mais em:

RANSOMWARE. **Avast**, 2016. Disponível em: <https://www.avast.com/pt-br/c-ransomware>. Acesso em: 8 ago. 2017.

O combate à criminalidade informática encontra vários entraves relacionados às lacunas legislativas, mas não somente a elas; também os relacionados aos reflexos que podem causar restrição à liberdade de expressão e ao acelerado desenvolvimento tecnológico. No Brasil, as leis específicas se tornarão obsoletas, acarretando na atipicidade de vários atos.

Reflita

A criação de mais normas penais específicas para punir os delitos informáticos traria uma solução para a crescente onda desse tipo de crime? Na sua opinião, uma repressão muito forte por parte do Estado inibiria a liberdade de expressão e a democracia? Leve em consideração o monitoramento da internet por parte de Agências de Inteligência como a NSA. Tais recursos são imprescindíveis para evitar ataques cibernéticos de larga escala (ciberterrorismo)?

Outro problema que traz a sensação de impunidade em relação aos delitos informáticos refere-se à falta de colaboração dos provedores de serviços. Estes, por sua vez, devem alertar e fixar, pela via contratual, a responsabilidade de seus usuários acerca das condutas delituosas que venham a ferir o ordenamento jurídico brasileiro, tornando claro o seu posicionamento na hipótese de consumação.

Todavia, felizmente existem aqueles provedores que colaboram com o poder público e com as vítimas dos delitos informáticos. Em razão dessa colaboração, a polícia tem conseguido reprimir alguns desses crimes.

É mundial a preocupação em buscar soluções para combater a criminalidade informática. Tanto é que, em 2001, o Conselho da Europa criou a Convenção de Budapeste para combate ao cibercrime, que entrou em vigor no ano de 2004, após a ratificação de cinco países. A *Convenção sobre o Cibercrime* tipifica os principais crimes cometidos no meio eletrônico e prioriza, conforme seu preâmbulo, uma política criminal comum, com o objetivo de proteger a sociedade por meio da adoção de legislação adequada e pela melhoria da cooperação internacional nesse campo.

A Convenção conta com a participação maciça de países europeus, reunindo diversos especialistas do mundo todo para tratar dessas questões. O Brasil, que aprovou pequenos ajustes no Código Penal e no Estatuto da Criança e do Adolescente, está na lista de países que poderiam integrar a convenção, porém, até o momento, optou por não o fazer.

Apesar disso, o Brasil possui, em determinados aspectos, leis mais rígidas, como a vedação ao anonimato prevista no artigo 5º, inciso IV, da Constituição Federal, porém é mais deficiente no tocante à capacidade de investigação (ferramentas técnicas, pessoal qualificado,

agilidade na resposta a incidentes), sobretudo em razão da falta de investimentos por parte do Estado.

Em razão disso, verificamos um crescimento exponencial no número de crimes informáticos. Além da citada sensação de impunidade e incapacidade investigativa, contribuem para tal fato, ao nosso ver: o crescimento no número de usuários de internet que não possuem uma cultura voltada ao uso seguro e consciente do meio digital; a lucratividade dos criminosos digitais, tendo em vista o número elevado de usuários despreparados; falta de conscientização de pessoas e empresas na área de segurança da informação, que enxergam tal fato como despesa, e não investimento, na crença de que nunca serão vítimas desse tipo de crime.

Como podemos ver, os desafios são enormes e inúmeros, todavia o Brasil possui plena capacidade para ocupar local de destaque no combate à criminalidade informática. Para tanto, devemos inovar e nos conscientizar do perigo de tais crimes e seus potenciais danos, tanto à população quanto ao Estado.

Sem medo de errar

Vistos os principais conceitos desta seção, vamos resolver nossa situação-problema (SP)?

Lembre-se, caro aluno, qde ue ao final da unidade devemos apresentar uma queixa-crime completa. Ao resolver nossa primeira situação-problema, estaremos elaborando a primeira parte da referida peça processual.

Retomando a SP, temos que, após realização de perícia no computador de uma jovem de 14 anos que teve fotos íntimas divulgadas na internet vinculadas a um site de pornografia infantil, descobriu-se que o número IP utilizado para invadir o dispositivo está vinculado a um provedor de conexão localizado na Argentina. De posse dessa informação, você enviou uma notificação extrajudicial ao provedor, inteirando-o da situação e requerendo os dados do titular daquele IP, o que foi prontamente atendido, tendo em vista a política de combate à pornografia infantil da empresa. Descobriu-se que o criminoso é brasileiro, mas que estava utilizando uma ferramenta de conexão privada (VPN) para mascarar o real local de sua conexão. Nesse caso, qual o juízo competente para se propor a queixa-crime, o brasileiro ou o argentino?

Antes de entrarmos na queixa-crime em si, vamos relembrar o que estudamos acerca da territorialidade do delito informático.

Quando tratamos de competência e lugar do crime informático, nos deparamos com algumas controvérsias. Como dissemos, determinar a territorialidade implica determinar o juiz competente para processar e julgar um delito informático. No que tange ao local do crime, o Código Penal adotou, em seu art. 6º, a teoria da ubiquidade, sendo considerado o lugar do crime o local onde ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria se produzir o resultado. Já no que diz respeito às condutas ilícitas praticadas em território estrangeiro, não se aplicariam as normas brasileiras, considerando a soberania do país, sendo que a questão deverá ser tratada pela extradição. No entanto, a autoridade brasileira é competente para processar um crime digital praticado por agente brasileiro no exterior, com vítima no Brasil, mas dependerá que esse agente adentre o território brasileiro.

Agora, iremos relembrar como elaborar uma queixa-crime:

EXCELENTÍSSIMO SENHOR DOUTOR JUIZ DA __ VARA CRIMINAL DA COMARCA XXXX/XXXX

(Espaço de 8 linhas)

FULANA, (qualificação), representada pela sua genitora, Sra. (...), vem, respeitosamente, perante à presença de Vossa Excelência, através de seu advogado infra-assinado, com escritório profissional (endereço), que a esta subscreve, com fulcro nos artigos 30, 41 e 44 do Código de Processo Penal, oferecer a presente **QUEIXA-CRIME**, contra SICRANO (qualificação), (endereço), pelos motivos que a seguir passa a expor:

I – DO FORO COMPENTENTE

Trata-se de delito informático em que a vítima, menor de idade, teve seu dispositivo computacional invadido por terceiro. Após realização de perícia no dispositivo invadido, descobriu-se que o

número IP (*Internet Protocol*) utilizado está vinculado a um provedor de conexão localizado na Argentina.

Diante do ocorrido, a vítima prontamente enviou uma notificação extrajudicial a este provedor (doc. Anexo), inteirando-o da situação e requerendo os dados do titular daquele IP, o que foi prontamente atendido, tendo em vista a política de combate à pornografia infantil da empresa.

Descobriu-se que o criminoso é brasileiro, mas que estava utilizando uma ferramenta de conexão privada (VPN) para mascarar o real local de sua conexão, que é na cidade de (...), estado de (...), no Brasil.

No que tange ao local do crime, o Código Penal adotou, em seu art. 6º, a teoria da ubiquidade, sendo considerado o lugar do crime o local onde ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria se produzir o resultado.

Nesse sentido, a autoridade brasileira é competente para processar um crime digital praticado por agente brasileiro no exterior, com vítima no Brasil. Portanto, competente o presente foro para julgar e processar a presente ação.

Avançando na prática

Classificação dos delitos informáticos

Descrição da situação-problema

Você, na condição de consultor jurídico, foi procurado por uma empresa de seguros para dar sua opinião legal acerca de um novo produto que ela pretende lançar no mercado. Trata-se de um seguro contra ataques cibernéticos, algo que a concorrência já está praticando. O produto ainda está em fase desenvolvimento, mas surgiu uma dúvida em relação aos tipos de crimes eletrônicos existentes em nossa legislação. Você deverá dar sua opinião legal sobre tal questionamento, levando em consideração, principalmente, a classificação doutrinária desse tipo de crime.

Resolução da situação-problema

Para resolver o questionamento proposto pela consulente, iremos levar em consideração o bem jurídico ofendido para, assim, podermos classificar os delitos informáticos.

Atualmente, a doutrina classifica tais crimes ou delitos em: delitos informáticos próprios; delitos informáticos impróprios; delitos informáticos mistos; delitos informáticos mediatos ou indiretos.

Os "delitos informáticos próprios" são aqueles em que o bem jurídico ofendido é a tecnologia da informação em si. Para esses delitos, a legislação penal era lacunosa, sendo que, diante da vedação às analogias no Direito Penal, muitas práticas não poderiam ser enquadradas criminalmente.

Os "delitos informáticos impróprios" são aqueles em que a tecnologia da informação é o meio utilizado para a agressão a bens jurídicos já tutelados pelo Código Penal. Para esses delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais.

Já os "delitos informáticos mistos" são os crimes complexos em que, além da proteção do bem jurídico informático, a legislação protege outro bem jurídico. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico.

Por último, os "delitos informáticos mediatos (ou indiretos)" são aqueles delitos informáticos praticados para a ocorrência de um delito não informático consumado ao final.

Faça valer a pena

1. Sobre os delitos informáticos, a Lei nº 12.737/2012, conhecida como "Lei Carolina Dieckmann", tipificou e atribuiu penas a algumas condutas, a fim de proteger determinados bens jurídicos que antes não eram tutelados pelo Direito Penal, como:

Assinale a única alternativa que completa corretamente a afirmação.

a) Dados informáticos com valor econômico.
b) A integridade dos dados informáticos, somente.
c) A privacidade do usuário, somente.
d) A privacidade e integridade dos dados informáticos.
e) A informática.

2. O dispositivo a seguir, retirado do Código Penal Brasileiro, trata do princípio da ubiquidade: "Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado" (BRASIL, 1940, art. 6º).
Caso um delito eletrônico tenha sido praticado por um indivíduo na cidade de Campinas/SP, que invadiu um computador localizado em Salvador/BA, qual a comarca competente para processamento e julgamento da ação penal?
a) Tanto Campinas/SP quanto Salvador/BA.
b) Campinas/SP.
c) Salvador/BA.
d) Deverá ser verificado onde se localiza o servidor em que estavam hospedados os dados.
e) Justiça Federal de Campinas/SP.

3. Imagine a seguinte situação: um *cracker* clona dados bancários de um cidadão brasileiro e realiza diversas compras internacionais. Em investigação policial, descobre-se que o *cracker* é brasileiro e reside em território europeu.
Analisando a situação descrita, assinale a opção mais correta para o caso.
a) São aplicadas as normas brasileiras, tramitando o processo independentemente da extradição do agente.
b) A questão deverá ser tratada pela extradição e aplicada a legislação brasileira quando o agente adentrar o território brasileiro.
c) O delito não poderá ser processado, por falta de competência da autoridade brasileira.
d) Não é possível a extradição nesse caso, por ser o agente brasileiro.
e) A autoridade brasileira é competente para julgamento e processamento da ação penal, mas será aplicada a legislação do país europeu.

Seção 4.2

A criança e o adolescente na internet sob a ótica criminal

Diálogo aberto

Como estudamos anteriormente, com a popularização da rede mundial de computadores, diferentes tipos de usuários passaram a frequentar o ciberespaço. Tal fato atraiu a atenção de agentes maliciosos, que viam o desconhecimento do usuário comum como fonte de oportunidade de ganhos. Ocorre que, muitas vezes, tais ganhos se baseiam em atos ilícitos, ou pior, na exploração de vulneráveis. Daí a necessidade de proteção por meio de uma legislação penal sólida. É o que veremos nesta seção.

Antes de apresentarmos nossa situação-problema, vamos relembrar nosso contexto de aprendizagem: você deverá elaborar uma queixa-crime em desfavor do titular do criminoso que invadiu o dispositivo de uma jovem, menor de idade que teve fotos íntimas divulgadas na internet, indo parar em um site de pornografia infantil.

Analisando as nuances do caso ocorrido, quais tipos penais previstos no Código Penal e no Estatuto da Criança e Adolescente poderiam ser utilizados para embasar nossa queixa-crime? Considere a possibilidade da ocorrência tanto de delitos informáticos próprios, quanto impróprios. Não se esqueça de fundamentar!

Esta será a segunda parte do nosso produto, a queixa-crime, onde você deverá dizer o direito, ou seja, o fundamento jurídico penal do pedido.

Para resolver essa questão, iremos estudar nesta seção o enquadramento das diferentes condutas ilícitas praticadas no meio eletrônico conforme os tipos penais previstos no Código Penal e legislação correlata, além das normas de proteção da criança e do adolescente contra crimes eletrônicos, sobretudo pornografia infantil.

Não pode faltar

Na seção anterior, estudamos brevemente a evolução dos delitos informáticos e sua classificação, em delitos informáticos próprios, impróprios, mistos e mediatos ou indiretos, a depender, sobretudo, do bem jurídico penalmente tutelado. Nesta seção, iremos aprofundar nossos estudos, analisando as condutas antijurídicas mais praticadas no meio eletrônico e classificando-as conforme o critério mencionado.

Optamos também por dar uma atenção especial aos crimes praticados contra a criança e o adolescente que, ao nosso ver, são aqueles mais graves e que ensejam um combate mais efetivo, visto que envolve a proteção jurídica de incapazes.

Sabemos que muitos dos crimes já existentes podem ser cometidos através do meio eletrônico, como os crimes contra a honra, estelionato, extorsão, pornografia infantil, entre outros. Isso ocorre por um simples motivo: as características do tipo penal se referem à conduta, ação ou omissão, e não necessariamente aos meios por onde tais crimes são praticados.

Esses tipos de conduta classificam-se como crimes informáticos impróprios ou mistos, ou mesmo mediatos. Iremos analisar mais detalhadamente tais delitos, nos restringindo àqueles que consideramos como os principais.

4.2.1 Crimes contra o patrimônio

Trata-se de modalidade que causa muita preocupação devido a sua frequente ocorrência. Entre as várias condutas, destacamos o furto, o estelionato, o dano e a extorsão.

Um dos crimes de maior frequência refere-se à conduta de criminosos que transferem quantias monetárias de contas de terceiros para suas próprias contas, utilizando ainda contas "fantasmas" para disfarçar o tráfego monetário. Temos ainda as fraudes informáticas, que se enquadram no crime de estelionato, em que os dados pessoais de um usuário são utilizados indevidamente para que o criminoso realize, por exemplo, empréstimos bancários, através da internet, em seu próprio benefício. Cite-se também o dano informático, em que o criminoso, por exemplo, acessa o sistema de uma empresa e deleta uma grande quantidade de informações vitais para o funcionamento dela.

Ademais, é importante salientar que o ano de 2017 foi marcado pela frequente ocorrência de uma prática ilícita que ficou conhecida como *ransomware*, ou sequestro de dados. Trata-se de prática que envolve o uso de um código malicioso (vírus) que restringe o acesso ao sistema informático, por meio de criptografia, seguido da exigência de um valor a título de resgate para que se permita o restabelecimento do acesso.

A prática do sequestro de dados pode ser enquadrada no crime de extorsão, ainda que o valor do resgate não seja pago, já que se trata de crime formal (independe de resultado).

4.2.2 Crimes contra a honra

Os crimes contra a honra, caro aluno, são condutas antijurídicas que denigrem a integridade moral das pessoas, podendo ser enquadradas nos crimes de calúnia, injúria ou difamação. Esse tipo de conduta ganhou novos contornos após o advento das redes sociais. É cada vez mais comum nos depararmos com casos de ofensas praticadas pela internet, mediante dizeres, fotos, imagens, desenhos, etc. Os crimes contra a honra, quando praticados no meio eletrônico, potencializam os danos causados à vítima, pois atingem uma infinidade de leitores.

Exemplificando

O alcance de um vídeo ofensivo após sua "viralização" na internet é praticamente incalculável. Trata-se de verdadeira ampliação do "espaço público" por onde os efeitos do crime poderiam percorrer. A título de exemplo, podemos citar o caso do garoto Nissim Ourfali, que teve sua imagem retratada em diversos vídeos ofensivos.

ARAÚJO, B.; SOTO, C. Nissim Ourfali: Justiça determina que Google tire do ar vídeos sobre garoto. **G1**, 16 mar. 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/03/nissim-ourfali-justica-determina-que-google-tire-do-ar-videos-sobre-garoto.html>. Acesso em: 17 ago. 2017.

4.2.3 Interceptação de correspondência

Trata-se de afronta direta ao preceito constitucional do sigilo à correspondência, sendo o ato de interceptar uma correspondência dirigida a certa pessoa. É conduta tipificada no artigo 151 do Código Penal. Trazendo tal conduta para o meio eletrônico, ela pode ocorrer pela violação do e-mail pessoal ou outro tipo de comunicação em que somente o destinatário deveria receber, com exclusividade. A

violação pode se dar não só pelo acesso, mas pela leitura, modificação ou ainda o uso dos dados contidos na mensagem.

4.2.4 Violação de direitos autorais

Os direitos autorais, como vimos na Unidade 3, são muito mais suscetíveis de violação com o emprego de meios eletrônicos, em especial a internet. Já virou lugar-comum a disseminação não autorizada de arquivos de áudio, vídeo, texto, fotos, etc. Especialmente no Brasil, não temos um apreço pelas criações de espírito, em que pese os direitos autorais serem penalmente resguardados. Todavia, o mau uso da tecnologia potencializa a violação desses direitos.

4.2.5 Pornografia infantil

Caro aluno, é necessário fazer um parêntese nesse tipo de crime, uma vez que é um dos principais focos de nossa seção. Iremos dedicar uma especial atenção, essencialmente porque se trata de conduta que talvez provoque a repulsa da sociedade. Não é possível aceitarmos as situações constrangedoras a que crianças e adolescentes são submetidas para saciar as fantasiais sexuais de pessoas desequilibradas.

Primeiramente, não podemos confundir a pornografia infantil com pedofilia. A pornografia infantil é crime previsto na Lei nº 8.069, de 13 de julho de 1990, conhecida como Estatuto da Criança e do Adolescente (ECA). Por sua vez, a pedofilia é uma doença, cujo portador sente-se atraído por crianças.

A Lei nº 11.829/2008 promoveu a alteração do ECA (Lei nº 8.069), incluindo o artigo 241-A, que assim dispõe:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.

> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. (BRASIL, 1990, artigo 241-A)

Outras condutas passaram a ser igualmente puníveis. Nesse sentido, não havia punição para o indivíduo que obtivesse qualquer material pornográfico envolvendo menores de 18 anos, com o objetivo único de guardar consigo. Porém, o art. 241-B definiu tal prática como delito, desde que demonstrado o dolo do agente. Assim, se uma pessoa recebe uma imagem pornográfica de menor de 18 anos por um aplicativo de mensagens e a armazena em seu dispositivo celular, poderia responder por tal crime.

Ato contínuo, temos o art. 241-C, que dispõe que simular a participação de criança ou adolescente em cenas de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual implica em ato criminoso. A lei, por sua vez, passou a alcançar não só as situações reais como também aquelas que envolvem outros tipos de imagens, como desenhos animados, pinturas, montagens, etc.

Embora sejam imagens fictícias, uma vez que mostram crianças sofrendo abusos sexuais, a sua divulgação por si só já constitui motivo suficiente para caracterizar ilícito penal. Salienta-se que a difusão dessas imagens fantasiosas serve como alimento para que abusos reais aconteçam, funcionam como meio de potencializar e estimular os sentimentos nutridos pelos pedófilos.

Por último, ressalte-se a norma contida no art. 241-E, que esclarece a expressão "cena de sexo explícito ou pornográfica" como "qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais".

Outra prática que vem assolando as crianças e os adolescentes atualmente é o *cyberbullying*, que nada mais é que o velho *bullying* transposto para o meio eletrônico. Trata-se da intimidação sistemática da vítima praticada principalmente pela internet. Nada mais é do que um crime contra a honra (calúnia, injúria ou difamação) praticado em meio virtual.

Apesar da punição prevista no Código Penal, o legislador ordinário nos contemplou com a Lei nº 13.185/15, apelidada de "Lei de Bullying". A referida lei estabelece a obrigação para escolas, clubes e agremiações de instituírem um "Programa de Combate à Intimidação Sistemática - *Bullying*".

Caso a instituição aja com negligência, não tomando medidas para prevenir a prática de *cyberbullying* entre seus alunos ou associados, ou mesmo fique inerte diante dessa ocorrência, poderá se complicar no Judiciário, suportando danos diversos, sobretudo de ordem financeira.

Pesquise mais

Para saber um pouco mais sobre a Lei do *Bullying*, sugerimos a leitura do seguinte artigo:

MESQUITA, A. P. S. L. Recém sancionada, lei de combate ao *bullying* é distante da realidade. **Consultor Jurídico**, 13 nov. 2015. Disponível em: <http://www.conjur.com.br/2015-nov-13/ana-paula-mesquita-lei-bullying-distante-realidade>. Acesso em: 17 ago. 2017.

Avançando em nossa didática, vimos os principais tipos penais que se classificam como delitos informáticos impróprios, ou ainda que, a depender do caso, podem ser considerados como mistos ou mediatos. Agora, iremos estudar alguns dos tipos penais que podemos classificar como delitos informáticos próprios, ou seja, aqueles cujo bem jurídico tutelado é o sistema informático em si.

Conforme estudado na Seção 4.1, vimos que com o advento da Lei nº 12.737/12 os primeiros delitos informáticos próprios foram tipificados em nossa legislação. Apelidada de "Lei Carolina Dieckmann", o referido diploma legal adveio do Projeto de Lei nº 2.793/2011. Vamos agora, caro aluno, analisar os tipos penais trazidos por essa lei.

4.2.6 Invasão de dispositivo informático

Previsto no artigo 154-A do Código Penal, o tipo penal resguarda a liberdade individual de manter íntegros os dados dispostos em preceito informático, bem como ilesos os próprios dispositivos em si, protegidos por mecanismo de segurança, contra acessos não autorizados, expressa ou tacitamente, com a finalidade de obter, alterar ou destruir dados, ou, ainda, instalar vulnerabilidades com fim de obter vantagem ilícita. Vejamos o que preceitua a norma legal:

> 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.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 1940, art. 154-A)

A lei estabelece, como condição para prática do delito, que o dispositivo invadido esteja protegido por "mecanismos de segurança", não estabelecendo quais mecanismos são considerados seguros. A ausência de mecanismo de segurança levaria à atipicidade do fato. Entretanto, a doutrina não é pacífica em definir o que poderia ser ou não considerado um mecanismo seguro. Existem aqueles que acreditam que qualquer tipo de mecanismo poderia ser considerado, inclusive uma senha padrão, como "admin" ou "1234". Outros,

consideram somente que os mecanismos verdadeiramente eficazes deveriam ser considerados para fins do referido artigo 154-A (JESUS, 2016, p. 88).

Trata-se de crime que se apura mediante ação penal pública condicionada à representação da vítima, salvo se for praticado contra a Administração Pública, caso em que a ação passará a ser incondicionada, nos termos do artigo 154-B do Código Penal. Ainda, considerando que a pena é inferior a dois anos, será processado em face do Juizado Especial Criminal. Lembrando que, a depender da complexidade técnica do delito, ou seja, havendo necessidade de realização de perícia técnica, tal competência poderá ser deslocada para a Justiça Comum.

4.2.7 Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Um dos principais delitos informáticos próprios cometidos no mundo cibernético é a indisponibilização de serviços, ou seja, ataques contra a intermitência de um serviço de tecnologia da informação. A principal técnica utilizada para esses ataques é a chamada, em inglês, *Denial of Service* (DoS), ou ataque de negação de serviços.

Assimile

Um ataque de negação de serviços é uma tentativa de tornar recursos de um sistema indisponíveis para quem os utiliza, sendo os alvos mais comuns os servidores web. Não se trata de invasão de sistema ou dispositivo informáticos, mas de nítida invalidação por sobrecarga.

Além do DoS, outra derivação desse ataque é *Distributed Denial of Service* (DDoS). Nessa modalidade, um computador "mestre" pode assumir o comando de centenas ou milhares de milhares de outras máquinas, os "zumbis", podendo ordenar que eles ataquem determinado alvo em certa data e hora. Essa modalidade é particularmente preocupante em razão do advento da tecnologia "Internet das Coisas" (IoT), tendo em vista a grande quantidade de dispositivos conectados à rede mundial de computadores. Não estamos mais falando de desktops ou laptops, mas de relógios, geladeiras, carros, ar-condicionado, etc.

O artigo 266 do Código Penal não era expresso ao tratar da possibilidade de sistemas informáticos serem objeto de interrupção.

Tal lacuna foi preenchida com a Lei nº 12.737/12, que complementou o dispositivo, que passou a vigorar com a seguinte redação:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública. (BRASIL, 1990, art. 266)

Trata-se de crime que se apura mediante ação pública incondicionada, cuja competência é do juízo comum, e não do Juizado Especial Criminal.

4.2.8 Falsificação de documento particular

A falsificação de documento particular ou alteração de documento particular verdadeiro já era considerada crime pelo artigo 298 do Código Penal, prevendo pena de reclusão de um a cinco anos e multa. O que a Lei nº 12.737/12 fez foi inserir um parágrafo onde equipara ao documento particular o cartão de crédito ou débito. Vejamos:

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
> Pena - reclusão, de um a cinco anos, e multa.
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (BRASIL, 2012, art. 298)

O escopo do legislador foi fazer frente às fraudes bancárias envolvendo clonagem de cartão. O agente que consegue romper a criptografia de um cartão legitimando-o ou, de certo modo, utilizando-o pode responder por tal crime. Ainda, trata-se de crime a ser apurado mediante ação penal pública incondicionada.

Reflita

Atualmente, a maioria da população utiliza cartões de débito e crédito consubstanciados em um verdadeiro pedação de plástico. Ocorre que

a tecnologia muda, torna-se obsoleta. Cada vez mais trabalhamos com certificados digitais, "carteiras virtuais", entre outros. Na sua opinião, referido tipo legal foi excessivamente específico ao indicar as tecnologias que se equiparam a documentos particulares? Será que o tipo legal já nasceu com prazo de validade atrelado à evolução tecnológica?

Concluindo, vimos que a antiga crença de que a internet seria uma terra sem lei está acabando. Não só porque tipos penais já consagrados no Código Penal de 1940 se aplicam às novas condutas praticadas pela internet, como também pelo fato de que tanto a sociedade quanto o legislador ordinário estão percebendo que novos bens penalmente tuteláveis estão surgindo, entre eles, a inviolabilidade de dados e sistemas informáticos.

Sem medo de errar

Ok! Vamos passar para a solução da nossa problemática apresentada no item *Diálogo aberto* desta seção. Você se lembra de que agora nosso desafio é elaborar uma queixa-crime em desfavor do titular do criminoso que invadiu o dispositivo de uma jovem, menor de idade?

Conforme disposto no início da seção, nossa situação-problema requer a análise sobre quais tipos penais previstos no Código Penal e no Estatuto da Criança e Adolescente poderiam ser utilizados para embasar nossa queixa-crime. Então, ao trabalho!

(2ª Parte da Queixa-crime)

DOS FATOS

(Descrever os fatos que levaram a vítima a buscar a tutela jurisdicional)

DO DIREITO

Conforme descrito nos fatos acima, a vítima, menor de idade, teve seu dispositivo computacional invadido, de maneira não autorizada

e mediante violação de dispositivo de segurança, no caso, o próprio *firewall* do dispositivo, sendo que o agente que praticou a conduta delituosa o fez com a finalidade de obter dados da vítima, no caso, fotos íntimas, posteriormente, divulgando-as na internet.

Tal fato, *a priori*, configura o crime de "invasão de dispositivo informático" contido no artigo 154-A do Código Penal, devendo o agente que praticou a conduta ser punido nos termos da referida norma legal, devendo ser ainda recebida a presente representação para posterior denúncia por parte do Ministério Público. Vejamos:

> 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.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 1940, art. 154-A)

Ainda, por ser a vítima menor de idade à época dos fatos, aplica-se *in casu* o Estatuto da Criança e do Adolescente e, consequentemente, seu artigo 241-A, que prevê punição pelo crime de pornografia infantil, uma vez que o agente praticou as condutas previstas no referido tipo legal, quais sejam, "oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente". Vejamos:

> Art. 241-A Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. (BRASIL, 1990, artigo 241-A)

Destarte, deve o Ministério Público, após apuração dos fatos e conclusão de eventual inquérito, proceder para com a denúncia do réu também pelo crime de pornografia infantil.

Avançando na prática

Ataques DDoS e seu enquadramento legal

Descrição da situação-problema

Você, na condição de advogado e consultor jurídico, foi procurado por representantes da Agência Nacional de Telecomunicações (Anatel) para dar sua opinião legal sobre recente caso ocorrido na empresa. Após a Agência emitir um comunicado de que estava estudando medidas para controle de franquia de dados de celulares,

o site da empresa foi atacado por um grupo de *crackers*, que causaram a indisponibilidade do site da instituição pelo prazo de 24 horas. Realizada a perícia, constatou-se que os criminosos utilizaram de um ataque DDoS para atacar os servidores da vítima. Assim, os representantes da Anatel pediram sua opinião legal com objetivo de saber se tal conduta poderia se enquadrar em algum tipo penal previsto em nossa legislação.

Resolução da situação-problema

Conforme consulta realizada pela Anatel, nos foi perguntado se o ataque realizado aos seus servidores, que provocaram a indisponibilidade temporária do site de sua titularidade, poderia se enquadrar em algum tipo penal previsto em nossa legislação.

Após realização de perícia pela consulente, constatou-se que os criminosos utilizaram de um ataque DDoS para atacar os servidores da vítima. Nesse tipo de ataque, um computador "mestre" pode assumir o comando de centenas ou milhares de milhares de outras máquinas, os "zumbis", podendo ordenar que eles ataquem determinado alvo em certa data e hora.

Tal conduta poderia se enquadrar no artigo 266 do Código Penal, que antes do advento da Lei nº 12.737/2012 não era expresso ao tratar da possibilidade de sistemas informáticos serem objeto de interrupção. Tal lacuna foi preenchida com referida lei, que complementou o dispositivo, que passou a vigorar com a seguinte redação:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública. (BRASIL, 1990, art. 266)

Trata-se de crime que se apura mediante ação pública incondicionada, cuja competência é do juízo comum e não do Juizado Especial Criminal. Portanto, a conduta descrita enquadra-se no tipo penal anteriormente citado.

Faça valer a pena

1. Analise a seguinte situação hipotética: um empregado de determinada empresa troca e-mails pessoais em seu local de trabalho. A empresa, além de verificar o ocorrido, leu todo o conteúdo dos e-mails do funcionário.
Enunciado: Assinale a única alternativa correta que indica qual delito eletrônico, em tese, poderia ter ocorrido nessa situação.
a) Interceptação de correspondência eletrônica.
b) Calúnia.
c) Dano.
d) Furto.
e) Violação de direitos autorais.

2. Segundo o Estatuto da Criança e do Adolescente, a conduta de oferecer, disponibilizar, trocar, publicar ou divulgar, por qualquer meio, inclusive o informático, vídeos ou fotos ou qualquer outro registro que contenha cenas de sexo explícito ou pornográfica envolvendo criança ou adolescente é considerada crime.
Assinale a única alternativa que indica corretamente de qual crime trata o texto.
a) Pedofilia.
b) Injúria.
c) Pornografia infantil.
d) Difamação.
e) Violação de dispositivo eletrônico.

3. Leia as assertivas a seguir sobre os delitos informáticos envolvendo crianças e adolescentes:
I – O porte de arquivos de mídia envolvendo cenas pornográficas de crianças não é crime.
II – A montagem de uma foto ou vídeo de sexo envolvendo crianças é crime.
III – A divulgação ou publicação de vídeos ou fotos de sexo explícito envolvendo crianças é crime.
Assinale a única alternativa que contém a assertivas corretas.
a) I, II e III.
b) I e II.
c) I e III.
d) II e III.
e) II.

Seção 4.3

Delitos informáticos e perícia computacional

Diálogo aberto

Caro aluno, até o momento estudamos os principais delitos informáticos previstos em nossa legislação. Todavia, existem algumas condutas que causam muita dúvida quanto ao seu enquadramento nos tipos penais previstos na Lei nº 12.737/2012. Assim, nesta seção, iremos estudar tais condutas, bem com algumas questões relacionadas à validade e obtenção de provas eletrônicas, além de alguns conceitos relacionados à computação forense.

Para tanto, iremos continuar trabalhando dentro do nosso contexto de aprendizagem que apresenta uma situação hipotética de invasão de dispositivo informático de uma jovem, menor de idade, com a consequente divulgação de imagens que denotam pornografia infantil.

Nesta seção, iremos considerar a seguinte situação-problema: restou constar, pela perícia realizada, que a invasão ao dispositivo da jovem vítima foi possibilitada pelo uso de uma versão desatualizada de um antivírus que foi incapaz de detectar o código malicioso usado para roubar as fotos. Diante disso, a invasão praticada poderia ser enquadrada no tipo penal previsto no artigo 154-A do Código Penal? Essa análise deverá constar na sua queixa-crime, de modo a facilitar o enquadramento da conduta tanto pelo MP quanto pelo juiz que receberá a denúncia.

Lembro a você, caro aluno, de que esta é nossa última seção e nela teremos de finalizar nosso produto, a queixa-crime envolvendo delito cometido por meio eletrônico. Nesta última parte, você deverá completar a parte referente ao fundamento jurídico da petição e o pedido final.

Para solucionar essa situação-problema, sua atenção deverá estar mobilizada para conteúdos como condutas informáticas que podem ou não ser consideradas crimes, além de breves considerações sobre perícia forense computacional.

Não pode faltar

Conforme estudamos na seção anterior, a Lei nº 12.737/2012 inovou ao criar certos tipos legais com objetivo de punir penalmente a prática de invasão de sistemas e dispositivos, entre outras condutas. Antes do advento da referida lei, era complicado punir determinadas condutas praticadas no meio eletrônico, essencialmente em razão do princípio da legalidade.

Os primeiros legisladores buscavam punir técnicas ou "armas" (códigos maliciosos), o que, ao nosso ver, se trata de um grande erro, pois as técnicas, artefatos e armas cibernéticas se modificam. Posteriormente, passaram a definir dezenas de comportamentos, uns até que coincidiam com outros, gerando uma espécie de "redundância criminal" (JESUS, 2016).

Em um terceiro momento, onde fora possível a aprovação de Leis de Crimes Informáticos, como a citada Lei nº 12.735/12, passou-se a dar relevância penal apenas a comportamentos considerados intoleráveis ou recorrentes na sociedade.

Por sua vez, comportamentos são relacionados a potenciais delitos informáticos próprios, em que a informática é o bem jurídico agredido. Logicamente, determinados comportamentos ofendem bens jurídicos diversos e podem ser realizados por intermédio da informática, conforme vimos na seção anterior. Trata-se dos delitos informáticos impróprios.

Todavia, existem alguns outros comportamentos ou condutas que poderão ou não ser considerados crimes. São casos análogos ao crime de invasão de dispositivo informático e outros, mas que, devido a suas peculiaridades, poderão ou não ser enquadrados nos tipos penais criados pela Lei nº 12.737/12. A seguir iremos enumerar algumas dessas condutas semelhantes, ou casos análogos.

4.3.1 Acesso ilegítimo

Trata-se de acesso sem autorização, não necessariamente com a violação de medidas ou mecanismos de segurança (invasão). Comumente, dá-se em um sistema informático que pode ser conceituado como um dispositivo isolado ou grupo de dispositivos interligados, em que um ou mais deles desenvolve o tratamento automatizado de dados.

Para se legislar sobre o acesso ilegítimo, é importante considerar que as convenções internacionais estabelecem que seja necessário indicar que tal acesso deve ter intenção ilegítima. Perceba que o artigo 154-A do Código Penal denota a violação de "mecanismos de segurança".

Reflita

Será que qualquer proteção poderia ser considerada um "mecanismo de segurança"? Qual sua opinião? Será que somente uma perícia técnica poderia dizer se o artefato existente em um dispositivo informático poderia ser considerado um mecanismo de segurança?

Cumpre esclarecer que tal mecanismo deverá estar protegendo o dispositivo daquela invasão específica. De nada adiantaria constatar a presença de um antivírus, se por padrão a máquina tem convite de assistência ou acesso remoto habilitado, que foram explorados. O mecanismo de segurança existente deve necessariamente ser violado (JESUS, 2016).

4.3.2 Interferência em sistemas

Está relacionada à conduta do agente que, dolosamente, causa obstrução grave, intencional e ilegítima ao funcionamento de um sistema informático, por meio da introdução, transmissão, danificação, eliminação, deterioração ou supressão de dados informáticos.

No Brasil, não temos um tipo que tutele os bens jurídicos de todas as condutas anteriormente narradas. Com a edição da Lei nº 12.737/2012, temos a tipificação do delito de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, que em verdade cobre apenas parte das condutas descritas.

4.3.3 Uso abusivo de dispositivos

Diz respeito à conduta de produzir, vender, obter, utilizar, importar ou distribuir dispositivo ou programa informático concebido para fins de prática de outras condutas criminosas ou mesmo senhas, códigos de acesso e dados informáticos que permitam o acesso indevido a sistemas. Com a publicação da Lei nº 12.737/2012, temos parte dessas condutas cobertas pelo artigo 154-A do Código Penal, em que a lei pune não só o invasor, mas aquele que desenvolve e distribui ferramentas com essa finalidade.

4.3.4 Furto de dados ou vazamento de informações

Consiste em copiar ou mover, indevidamente, informações protegidas ou confidenciais. Para punir a cópia indevida, muitas autoridades enquadravam a cópia indevida como crime de concorrência desleal, nos termos do artigo 195 da Lei nº 9.279/96, o qual estudamos na Unidade 3. Tal enquadramento é, no mínimo, forçado, esbarrando no princípio da legalidade e vedação a analogias *in malam partem*.

Assimile

Analogia *in malam partem* é a utilização da analogia em prejuízo do réu, pois cria figura criminosa, por similitude, a uma situação fática que não se encaixa, primariamente, em nenhum tipo incriminador. É proibida a sua utilização no campo penal por lesar a legalidade. No setor processual penal, admite-se o emprego da analogia com o objetivo de suprir lacunas, seguindo-se o disposto pelo art. 3º do Código de Processo Penal (NUCCI, 2016).

A Lei nº 12.737/2012 caracteriza o vazamento de informações como uma qualificadora do crime de "invasão de dispositivo informático", devendo a pena ser aumentada quando da invasão ocorrer a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas.

4.3.5 Pichação informática ou *defacement*

Trata-se de conduta praticada por agente que indevidamente altera o layout de páginas eletrônicas, websites, entre outros, promovendo sua "pichação", por meio da inclusão de textos ou figuras indevidas no código do site ou mesmo no banco de dados (onde também temos uma conduta de acesso indevido). Na maioria das vezes, o *defacement* (ou *deface*) pressupõe uma invasão, a qual, por si só, poderia ser punida nos termos do artigo 154-A do Código Penal. Por outro lado, a pichação, em si, pode caracterizar crime de dano.

Exemplificando

Recentemente, temos testemunhado um aumento das práticas de deface nos sites oficiais de órgãos do governo, sobretudo como forma de protesto aos escândalos políticos que abalam nosso país. A título de exemplo, citamos o ataque ocorrido em 11 de junho de 2017, no site do

governo federal, contra a imagem do então presidente Michel Temer.

PAYÃO, Felipe. Ataque hacker desfigura site do DF e tem Michel Temer como alvo. **TecMundo**, 12 jun. 2017. Disponível em: <https://www.tecmundo.com.br/ataque-hacker/117657-ataque-hacker-desfigura-site-df-tem-michel-temer-alvo.htm>. Acesso em: 21 ago. 2017.

Concluindo, vimos que, independentemente de seu enquadramento legal, diversas são as condutas nocivas praticadas no meio eletrônico. Nesse sentido, tal enquadramento é, por vezes, uma tarefa difícil, até para os especialistas no assunto. Isso ocorre não somente em razão da escassa jurisprudência sobre o tema, mas também pelas peculiaridades técnicas envolvidas.

Embora a análise do delito seja feita levando-se em consideração o bem jurídico atingido, devemos analisar também as ferramentas utilizadas, que servem de suporte para o correto enquadramento da conduta delituosa praticada. Se não bastasse, a coleta de provas eletrônicas também é diversa daquela das provas físicas, pois os documentos eletrônicos demandam um procedimento de obtenção muito mais técnico e cuidadoso, de modo a não contaminar toda a cadeia de custódia daquela prova.

Pesquise mais

A preservação das fontes de prova é, portanto, fundamental, principalmente quando se trata de provas cuja produção ocorre "fora do processo", como é o caso da coleta de DNA, interceptação telefônica, etc. Sobre a importância da cadeia de custódia, recomendamos a leitura do seguinte artigo:

LOPES JR, A.; ROSA, A. M. A importância da cadeia de custódia para preservar a prova penal. **Consultor Jurídico**, 16 jan. 2015. Disponível em: <http://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal>. Acesso em: 22 ago. 2017.

É de se notar que a cada dia diminui o receio em se admitirem como prova judicial os documentos eletrônicos, sobretudo em razão de sua segurança, ampla utilização, lastro legislativo e jurisprudência favorável. Aliás, a Lei nº 13.105/2015 ("Novo Código de Processo Civil") veio a reforçar tal ideia, dedicando uma seção específica para tratar sobre o tema, senão vejamos:

> Art. 439. A utilização de documentos eletrônicos no processo convencional dependerá de sua conversão à forma impressa e da verificação de sua autenticidade, na forma da lei.
> Art. 440. O juiz apreciará o valor probante do documento eletrônico não convertido, assegurado às partes o acesso ao seu teor.
> Art. 441. Serão admitidos documentos eletrônicos produzidos e conservados com a observância da legislação específica. (BRASIL, 2015, arts. 439 a 441)

Em que pese a ampla validade desse tipo de prova, percebemos um certo "preconceito" por parte de alguns em relação às provas eletrônicas, ao nosso ver devido ao sentimento de insegurança quanto àquilo que não se conhece.

Em virtude do uso massivo de computadores, a prova eletrônica pode e deve ser utilizada. Todavia, dificilmente alcançaremos a certeza inequívoca de confiabilidade, tanto no sistema eletrônico quanto no tradicional, ou em outro qualquer, mas, ainda assim, é possível imprimir uma confiabilidade necessária para a concretização de negócios jurídicos nesses meios.

Pode-se afirmar que a tecnologia trouxe mais ferramentas para a validação jurídica das provas, algo que se busca há muito, e hoje, por certo, já há força legal muito maior numa prova composta por um e-mail do que apenas um testemunho oral, por exemplo. O mesmo vale para uma assinatura digital ou biométrica do que apenas um RG ou CPF anotados à mão sem conferência do documento, ou cuja foto, normalmente, está desatualizada.

Portanto, admitindo-se a validade das provas eletrônicas, resta a questão da sua obtenção. Nesse sentido surge a perícia forense computacional, cuja finalidade é justamente conseguir provas que comprovem determinadas situações em eventual procedimento judicial. De forma geral, a perícia forense computacional extrai dos equipamentos informáticos os dados e informações relevantes para apuração de um fato, tal como a celebração de um negócio jurídico, a prática de um ilícito, etc.

Assimile

A Computação Forense é a ramificação da criminalística que tem como objetivo a análise de vestígios cibernéticos, englobando os elementos que os orbitam. Esse aspecto a torna uma área multidisciplinar (VELHO, 2016).

A perícia forense computacional pode ser dividida em quatro etapas:

- obtenção e coleta de dados;
- identificação de indícios;
- preservação de provas; e
- análise pericial.

Então, vamos verificar os detalhes de cada uma delas. Primeiramente, as provas devem ser obtidas de maneira legal, preferencialmente subsidiadas por um mandado de busca e apreensão ou outra forma de autorização judicial, bem como devem respeitar as leis e direitos dos usuários. Lembrando que uma prova obtida ilegalmente poderá invalidar todo um processo judicial, em razão da teoria do "fruto da árvore envenenada".

Assimile

A teoria dos frutos envenenados repreende a obtenção de provas ilícitas por derivação. Essa prova contamina as provas subsequentes, por efeito de repercussão causal, e o efeito é a nulidade do processo penal; eis que jamais se admite condenar o agente da infração penal sem observar as garantias constitucionais (ANDRADE, 2008).

Quanto à identificação de indícios digitais, cada tipo de conduta possibilita um tipo de evidência. Os indícios residentes em uma mídia podem ser relacionados para criar uma evidência que indique a ocorrência de um crime ou auxilie a identificação de um criminoso. Por exemplo, no caso de crime de pornografia infantil praticado pela internet, buscam-se imagens armazenadas no disco rígido, arquivos deletados, histórico de navegação, arquivos temporários, etc.

A preservação das provas está relacionada ao local de realização do ato ou da prática de crime e as provas nele encontradas. No caso de um delito, os primeiros a chegarem à cena do crime devem tomar

precauções para que se possa garantir a integridade dos indícios digitais, tentando não modificar arquivos ou desligar equipamentos. Isto porque muitos criminosos podem instalar códigos maliciosos que programem a destruição de arquivos quando desligados ou manipulados incorretamente. As provas devem ainda ser devidamente protegidas contra eventuais danos, tais como aqueles causados por altas temperaturas ou campos magnéticos.

Por fim, temos a fase da análise pericial, que compreende a pesquisa propriamente dita, onde o perito se detém especificamente nos elementos relevantes ao caso em questão. O processo de análise pericial pode ser dividido em duas camadas: análise física e análise lógica. A análise física é a pesquisa de sequências e a extração de dados de toda a imagem pericial. Já a análise lógica consiste em analisar os arquivos das partições. O sistema de arquivos é investigado de forma a percorrer os diretórios do objeto periciado.

Além das etapas da perícia forense computacional, cumpre fazermos algumas breves considerações sobre as fontes de informação da perícia. Ela busca indícios inicialmente por meio de uma varredura minuciosa no sistema computacional para verificar as informações contidas nele.

Existem três tipos de espaços que podem conter informações valiosas em um dispositivo informático: o arquivo lógico, que são blocos do disco rígido que estão atribuídos a um arquivo ativo ou à estrutura de contabilidade do sistema de arquivo; o espaço subaproveitado, formado por blocos do sistema de arquivos parcialmente usados pelo sistema operacional; e o espaço não locado, ou seja, quaisquer setores não tomados, que estejam ou não em uma partição ativa (FREITAS, 2013).

A maior fonte de informações para a perícia digital são os "sistemas de arquivos" e os "diretórios de configurações e de usuários". Como um banco de dados, o sistema de arquivos é a parte do sistema operacional responsável por organizar as informações do disco na forma de arquivos.

Outra fonte importante são os logs, pois permitem a reconstituição de fato que ocorrera no sistema computacional. Os logs registram informações das atividades dos usuários, dos processos e do sistema, as conexões e atividades na internet ou intranet.

Temos também os arquivos temporários, que são arquivos de texto ou até os que manipulam banco de dados, e que servem como diretórios de "rascunho" para todo o sistema. Esses arquivos são apagados automaticamente ao final da sessão de trabalho.

Dessa maneira, temos que os procedimentos de computação forense são fundamentais tanto na obtenção de provas eletrônicas para, por exemplo, instruir um processo judicial, quanto no processo de enquadramento legal de determinadas condutas nos tipos penais previstos em nossa legislação, sendo fundamental a apuração das ações praticadas pelo agente e o resultado prático delas.

Sem medo de errar

Vistos os conteúdos desta seção, vamos resolver nossa situação-problema?

Conforme colocado anteriormente, restou constatado pela perícia realizada que a invasão ao dispositivo da jovem vítima foi possibilitada pelo uso de uma versão desatualizada de um antivírus que foi incapaz de detectar o código malicioso usado para roubar as fotos.

Diante desse cenário, devemos analisar se a conduta praticada pelo agente se enquadra no tipo penal previsto no artigo 154-A do Código Penal, que tipifica o crime de invasão de dispositivo informático. Lembrem-se de que devemos responder essa questão na forma de queixa-crime, que é o produto desta unidade. Na verdade, trata-se de verdadeiro aprofundamento do tópico sobre invasão de dispositivo informático que compõe a segunda parte da queixa-crime e que elaboramos na Seção 4.2. Assim, o tópico deverá ser estruturado da seguinte forma:

(3ª Parte da Queixa-crime)

DOS FATOS

(Descrever os fatos que levaram a vítima a buscar a tutela jurisdicional)

DO DIREITO

Conforme descrito nos fatos acima, a vítima, menor de idade, teve seu dispositivo computacional invadido, de maneira não autorizada e mediante violação de dispositivo de segurança, no caso, o *firewall* do dispositivo, sendo que o agente que praticou a conduta delituosa o fez com a finalidade de obter dados da vítima, no caso, fotos íntimas, posteriormente, divulgando-as na internet.

Tal fato, *a priori*, configura o crime de "invasão de dispositivo informático" contido no artigo 154-A do Código Penal, devendo o agente que praticou a conduta ser punido nos termos da referida norma legal, devendo ser ainda recebida a presente representação para posterior denúncia por parte do Ministério Público. Vejamos:

> 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.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;

> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 1940, art. 154-A)

Em que pese a perícia computacional ter encontrado uma versão desatualizada do antivírus no computador da vítima, tal fato não tem o condão de desconfigurar o tipo penal citado. A uma, porque o *firewall* do sistema estava devidamente ativado, mostrando a preocupação da vítima em proteger seus dados. Segundo, o mecanismo de antivírus estava protegendo o dispositivo contra diversas modalidades de invasão, tendo em vista que a vítima não realizou alteração nos padrões de proteção do *software*.

PEDIDO

Por todo o exposto, requer-se:

- Seja designada audiência preliminar, na forma do artigo 72 da Lei nº 9.099/95 (Lei dos Juizados Especiais) para eventual composição e transação penal e, em caso de impossibilidade de conciliação, requer seja recebida a presente, CITADA o querelado para responder aos termos da ação penal; e não sendo o mesmo encontrado, sejam os autos enviados para a Justiça Criminal Comum, a fim de citá-la por edital, bem como para realização da instrução processual;

- A intimação do Ilustre Representante do Ministério Público para se manifestar no feito, nos termos do artigo 45 do Código de Processo Penal;

- A intimação e oitiva das testemunhas abaixo arroladas;

- Após confirmada judicialmente a autoria e materialidade dos delitos dos autos, seja o querelado condenado, julgando-se procedente a presente Queixa-Crime.

Protesta provar o alegado por todos os meios de prova admitidos em Direito inseridos nesta exordial, como também especialmente pela juntada posterior de documentos, ouvida do noticiado, depoimentos das testemunhas abaixo arroladas, perícias, diligências e tudo mais que se fizer necessário para a prova real no caso "*sub judice*".

- Apresentação do rol de testemunhas: x, y, z.

Termos em que
Pede deferimento

(Local e data)
(assinatura do advogado)

Avançando na prática

Deface como forma de protesto

Descrição da situação-problema

Você, na condição de advogado, foi consultado para dar seu parecer técnico jurídico sobre um incidente envolvendo seu antigo cliente, o senador Américo Embromão. O senador teve sua página pessoal na internet "vandalizada". Alguém alterou os códigos da página para que, no lugar da foto do deputado, constasse uma imagem contendo uma mala cheia de cédulas monetárias. Tal fato ocorreu logo após ser noticiado nos veículos de comunicação que o senador teria recebido propina de uma empresa de construção civil. Você deverá analisar se o caso em tela se enquadra em algum crime previsto em nossa legislação.

Resolução da situação-problema

Analisando o caso em tela, percebe-se que o consulente teve sua página pessoal supostamente invadida por terceiro que, por sua vez, teria alterado o layout da página de modo a causar danos à sua reputação e imagem.

Primeiramente, recomenda-se a realização de perícia forense computacional, de modo a verificar se a alteração do layout da página foi precedida de uma invasão ao sistema ou dispositivo da consulente,

ou se foi feito por pessoa com acesso a tais recursos, o que seria no caso um fortuito interno. Entretanto, caso verificada a invasão, a conduta amolda-se ao crime previsto no artigo 154-A do Código Penal, devendo o consulente apresentar queixa-crime caso deseje a punição do agente. Ainda, a inserção de imagem contendo uma mala cheia de cédulas monetárias configura também crime contra honra, ao passo que atribui a pecha de corrupto ao consulente.

Faça valer a pena

1. O furto de dados ou o vazamento de informações até o momento não é uma conduta tipificada pela legislação penal brasileira. No entanto, algumas autoridades têm enquadrado referida conduta como crime de concorrência desleal, previsto na Lei nº 9.279/96.
Sobre a situação descrita, assinale a única alternativa correta.
a) É admitido o uso da analogia na esfera penal.
b) Foi realizada analogia *in malam partem*, que viola o princípio da legalidade.
c) Na esfera do direito penal, o princípio da legalidade pode ser mitigado, tipificando condutas não descritas na norma penal.
d) Não é permitido o uso da analogia em direito penal, mas apenas dos costumes.
e) A conduta descrita poderia ser tipificada por decreto.

2. "Sites do governo do Distrito Federal foram invadidos por hackers e adulterados com imagens e textos de oposição ao presidente Michel Temer neste domingo (11). A Casa Civil do governo local diz que solucionou o problema no mesmo dia mas, nesta segunda (12), sites de busca ainda mostravam ofensas direcionadas a Temer, vinculadas ao portal oficial do governo do DF." (HANNA, 2017)
Analisando o texto, assinale a alternativa que indica corretamente a denominação da conduta descrita.
a) Interferência em sistemas.
b) Uso abusivo de dispositivos.
c) Vazamento de informações.
d) Furto de dados.
e) Pichação informática.

3. Sobre as provas eletrônicas, analise as assertivas a seguir:
I – O procedimento de obtenção de provas eletrônicas é o mesmo das provas físicas;
II – Ainda há um certo preconceito em relação ao uso das provas eletrônicas;

III – A Perícia Computacional pode extrair dados relevantes para a apuração de fatos discutidos em um processo.

Assinale a única alternativa que contém apenas assertivas corretas.

a) I.
b) I e II.
c) II e III.
d) I e III.
e) I, II e III.

Referências

ANDRADE, Camila. **Que se entende pela teoria dos frutos da árvore envenenada - "fruits of the poisonous tree?"** set. 2008. Disponível em: <https://lfg.jusbrasil.com.br/noticias/107553/que-se-entende-pela-teoria-dos-frutos-da-arvore-envenenada-fruits-of-the-poisonous-tree-camila-andrade>. Acesso em: 5 set. 2017.

ARAÚJO, B.; SOTO, C. Nissim Ourfali: Justiça determina que Google tire do ar vídeos sobre garoto. **G1**, 16 mar. 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/03/nissim-ourfali-justica-determina-que-google-tire-do-ar-videos-sobre-garoto.html>. Acesso em: 17 ago. 2017.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Diário Oficial da União, Brasília, 31 dez. 1940.

_____. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**, Brasília, 16 jul. 1990.

_____. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União, Brasília, 30 nov. 2012.

_____. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Diário Oficial da União, Brasília, 17 mar. 2015.

FREITAS, Andrey Rodrigues de. **Perícia forense aplicada à informática**. 2013. Monografia (Especialização em Internet Security)–IBPI, 2013.

HANNA, W. Hackers invadem sites do governo do DF e publicam ataques a Michel Temer. **G1**, 12 jun. 2017. Disponível em: <https://g1.globo.com/distrito-federal/noticia/hackers-invadem-sites-do-governo-do-df-e-postam-ataques-a-michel-temer.ghtml>. Acesso em: 21 set. 2017.

JESUS, Damásio de. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

LOPES JR, A.; ROSA, A. M. A importância da cadeia de custódia para preservar a prova penal. **Consultor Jurídico**, 16 jan. 2015. Disponível em: <http://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal>. Acesso em: 22 ago. 2017.

MESQUITA, A. P. S. L. Recém sancionada, lei de combate ao *bullying* é distante da realidade. **Consultor Jurídico**, 13 nov. 2015. Disponível em: <http://www.conjur.com.br/2015-nov-13/ana-paula-mesquita-lei-bullying-distante-realidade>. Acesso em: 17 ago. 2017.

NUCCI, Guilherme. **Analogia *in malam partem***. 25 ago. 2016. Disponível em: <http://www.guilhermenucci.com.br/dicas/analogia-in-malam-partem>. Acesso em: 28 ago. 2017.

PAYÃO, Felipe. Ataque hacker desfigura site do DF e tem Michel Temer como alvo. **TecMundo**, 12 jun. 2017. Disponível em: <https://www.tecmundo.com.br/ataque-hacker/117657-ataque-hacker-desfigura-site-df-tem-michel-temer-alvo.htm>. Acesso em: 21 ago. 2017.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Saraiva, 2015.

RANSOMWARE. **Avast**, 2016. Disponível em: <https://www.avast.com/pt-br/c-ransomware>. Acesso em: 8 ago. 2017.

TEIXEIRA, Tarcísio. **Curso de direito e processo eletrônico**: doutrina, jurisprudência e prática. 3. ed. atual. e ampl. São Paulo: Saraiva, 2015.

VALLE, J. D. Lei Carolina Dieckmann entra em vigor nesta terça-feira. **Veja**, 2 abr. 2013. Disponível em <http://veja.abril.com.br/tecnologia/lei-carolina-dieckmann-entra-em-vigor-nesta-terca-feira/>. Acesso em: 8 ago. 2017.

VELHO, Jesus Antônio. **Tratado de Computação Forense**. Campinas: Millennium Editora, 2016.

Anotações

Anotações

Anotações

Anotações

Anotações

ISBN 978-85-522-0213-4