KLS

Direito eletrônico e internet

Direito eletrônico e internet

Frederico Félix Gomes

Dados Internacionais de Catalogação na Publicação (CIP)

Gomes, Frederico Félix
G633d Direito eletrônico e internet / Frederico Félix Gomes. –
Londrina : Editora e Distribuidora Educacional S.A., 2016.
184 p.

ISBN 978-85-8482-700-8

1. Internet - Legislação. I. Título.

CDD 343

2016
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 não passava de um projeto? Que o termo "globalização" era impensável? Ou ainda, que a transmissão de dados por fibra óptica não passava de uma simples ideia?

Ao longo desse período, nossa sociedade passou por transformações drásticas. A informação, que era um bem caro, pouco acessível e centralizado passou a ser barata, extremamente acessível e compartilhada. Essa mudança de paradigma trouxe transformações em vários segmentos da sociedade, inclusive no Direito. Precisamos, assim, refletir quanto à forma como este é pensado e exercido.

Nosso estudo em Direito Eletrônico e internet objetiva 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 antigos conceitos do Direito.

Na Unidade 1, iremos estudar a evolução da sociedade rumo a uma "Sociedade da Informação", o surgimento do Direito Eletrônico, seus fundamentos e principais características, sua relação com outros ramos jurídicos e a problemática relacionada à regulação do espaço virtual, além da prova de autoria dos atos no meio digital. Na Unidade 2, analisaremos o confronto entre direitos fundamentais na internet, bem como a responsabilidade dos provedores, especialmente pelos atos de terceiros. Na Unidade 3, estudaremos questões ligadas à proteção da propriedade intelectual na internet, em face dos novos modelos de negócios on-line. Por fim, na Unidade 4 analisaremos os problemas ligados ao cibercrime.

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

Fundamentos do direito eletrônico

Convite ao estudo

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

Ao longo desse período, nossa sociedade passou por transformações drásticas. A informação, que era um bem caro, pouco acessível e centralizado passou a ser barata, extremamente acessível e compartilhada. Essa mudança de paradigma trouxe transformações em vários segmentos da sociedade, inclusive no Direito. Precisamos, assim, refletir quanto à forma como este é pensado e exercido.

Nosso estudo em Direito Eletrônico e internet objetiva 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 antigos conceitos do Direito.

Para tanto, consideremos a seguinte Situação Geradora de Aprendizagem (SGA): Suponhamos que você foi contratado por uma empresa do ramo de cosméticos para construir toda sua plataforma de e-commerce onde irá vender seus produtos aos seus consumidores. A empresa pediu que o site fosse construído em conformidade com as leis que regulam a internet e o comércio eletrônico, e ainda, que também restasse garantida a segurança das transações e veracidade dos dados do consumidor. Diante desse cenário, pergunta-se: Quais leis se aplicam à internet? É necessária a criação de leis específicas para regulação do espaço virtual? Como garantir a veracidade das informações prestadas pelo consumidor? Como criar rotinas sistêmicas capazes de preservar

dados que poderão ser usados pela empresa em caso de ações na justiça?

Iremos analisar, a cada seção de autoestudo, um aspecto desse problema. Na Seção 1.1, iremos estudar a evolução da sociedade rumo a uma "Sociedade da Informação", o surgimento do Direito Eletrônico, bem como seus fundamentos e principais características. Na Seção 1.2 analisaremos o conceito de Direito Eletrônico, sua relação com outros ramos jurídicos e a problemática relacionada à regulação do espaço virtual. Na Seção 1.3, desvendaremos o fenômeno da desmaterialização dos documentos, além da prova de autoria dos atos no meio digital. Na Seção 1.4, exploraremos o conceito de identidade digital, a evolução do modelo de identificação até o uso da certificação digital e a segurança jurídica nas relações entre ausentes.

Seção 1.1

Rumo à sociedade da informação: a importância da internet e o surgimento do Direito Eletrônico

Diálogo aberto

Você sabia que a internet foi concebida originalmente como um projeto de caráter militar? Em 1969, uma rede de computadores denominada ARPANET, criada pelo Departamento de Defesa dos Estados Unidos, funcionava por meio da tecnologia *packet switched* (comutação por pacotes de dados). Inicialmente tais computadores utilizavam o protocolo NCP (*Network Control Protocol*), porém este apresentava significativa perda de pacotes durante a transmissão de dados. Surgiu daí a necessidade de adotar um protocolo de comunicação mais eficiente e confiável. Então, criou-se o protocolo TCP/IP, que é até hoje utilizado, estando em sua sexta versão (IPv6).

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, na própria evolução humana rumo à "Sociedade da Informação". A internet trouxe muitas facilidades que permitiram a interligação de empresas e pessoas localizadas em diferentes locais. Relembramos aqui nossa Situação Geradora de Aprendizado: Suponhamos que você foi contratado por uma empresa do ramo de cosméticos para construir toda sua plataforma de e-commerce onde irá vender seus produtos aos seus consumidores. A empresa pediu que o site fosse construído em conformidade com as leis que regulam o comércio eletrônico, e que também restasse garantida a segurança das transações e veracidade dos dados do consumidor. Diante desse cenário, que estará presente em toda esta Unidade de Ensino, você, com base nos estudos iniciais sobre Direito Eletrônico, deverá resolver o seguinte problema: quais elementos de um ato jurídico, como a compra de uma mercadoria, merecem especial atenção quando realizado por meio da internet?

Para solucionar o problema proposto para essa Seção 1.1, você deverá

considerar os principais desafios enfrentados pelo Direito face ao advento de novas tecnologias, sobretudo no tocante ao local do ato, o tempo do ato e a lei aplicável às partes que celebraram o ato pela internet.

Não pode faltar

A primeira metade da década de 1990 marcou não só a utilização da rede pelas pessoas em geral, como também a publicação dos primeiros artigos e textos jurídicos sobre a aplicação do direito à internet. As primeiras discussões envolveram, principalmente, os problemas relacionados aos conflitos de jurisdição no espaço virtual. Em razão da possibilidade de pessoas acessarem websites localizados em outros países e praticarem atos jurídicos, tais como jogos em cassinos, fora de seus países de origem, o problema da jurisdição foi o mais estudado e analisado à época.

Pesquise mais

O filósofo francês Pierre Levy muito nos ensinou sobre o processo da "virtualização". Segundo o autor, a virtualização não implica na perda da realidade, mas sim a mudança de seu eixo de gravidade. Ou seja, uma empresa virtualizada apresenta novos e diferentes problemas. Você concorda com esse ponto de vista? Quer saber mais? Leia a seguinte obra: LÉVY, Pierre. **O que é virtual?** São Paulo: Ed. 34, 1996.

O chamado "Direito Tradicional" não conseguia resolver essa e outras questões, surgindo daí a necessidade de um ramo jurídico diferenciado, marcado notadamente pela necessidade de conhecimentos técnicos sobre conceitos computacionais e sobre a própria estrutura da rede mundial de computadores. Nasceu, a partir daí, o "Direito Eletrônico", conhecido também como "Direito Digital" ou "Direito Virtual". Conforme ensinamento do professor Carlos Alberto Rohrmann, "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).

Reflita

Você acredita que nosso sistema jurídico atual precisa realmente de um ramo específico para tratar dessas novas questões tecnológicas? Ou os ramos tradicionais do direito, como o cível, penal e constitucional são capazes de solucionar todos esses novos conflitos?

As primeiras pesquisas do Direito Eletrônico foram, pois, associadas ao fenômeno da "desterritorialização", que permitiu a formação de grupos sem as pessoas deixarem o conforto de suas casas. Uma vez que a virtualização acarretou esta "desterritorialização" das relações humanas e, consequentemente, das relações jurídicas, um problema inicialmente levantado foi a aplicação do direito aos atos e fatos jurídicos aperfeiçoados em meio virtual. Tal preocupação decorre da característica do direito ser essencialmente territorial.

Assimile

O direito interno normalmente aplica-se dentro dos limites geográficos do território de determinado Estado. A extraterritorialidade da aplicação da lei é exceção à regra geral. Tal exceção faz sentido por vários motivos, tais como o conhecimento e o entendimento do direito nacional por parte daquelas pessoas que vivem em determinado Estado nos limites territoriais de outro, bem como a reação adversa de um Estado quando seus nacionais são julgados por tribunais estrangeiros.

Outra questão interessante diz respeito ao elemento "tempo". Toda norma tem um elemento tempo determinado, chamado "vigência", que se refere à duração dos efeitos de uma norma no ordenamento jurídico. No entanto, o elemento tempo no Direito Eletrônico extrapola o conceito de vigência e abrange a capacidade de resposta jurídica a determinado fato. Conforme Patrícia Peck Pinheiro, esse tempo pode ter uma relação ativa, passiva ou reflexiva com o fato que ensejou sua aplicação, ou seja, com o caso concreto (PINHEIRO, 2013, p. 81).

O tempo ativo se refere àquele em que a velocidade de resposta da norma pode implicar no próprio esvaziamento do direito subjetivo. Como exemplo, podemos citar o caso de uma empresa que necessita que um contrato de tecnologia seja cumprido e seja feito o upgrade em seus equipamentos. Se ele não encontrar uma velocidade de aplicação, pode significar não só a obsolescência do que está pleiteando como o seu esvaziamento (PINHEIRO, 2013, p. 81).

Exemplificando

Foi o que aconteceu à época do bug do milênio, em que a discussão de quem deveria ou não ser responsável pela modificação dos códigos não poderia ultrapassar a data da virada do ano, pois os efeitos seriam irremediáveis. Por sorte, nada de mais grave aconteceu, mas muitas empresas não conseguiram valer seus contratos de tecnologia e arcaram com custos sozinhas.

O tempo passivo é aquele explorado principalmente pelos agentes delituosos, que acreditam que a morosidade jurídica irá desencorajar a parte lesada de fazer valer seus direitos. Por sua vez, o tempo reflexivo é aquele que opera de modo ativo e passivo, simultaneamente, provocando efeitos em todos aqueles conectados ao espaço virtual. É o caso de determinados crimes praticados na internet, como pedofilia e pirataria (PINHEIRO, 2013, p. 81).

Assim, o elemento tempo é determinante para estabelecer obrigações e limites de responsabilidade entre as partes, quer seja no aspecto de contratos, serviços, direitos autorais, quer seja na própria credibilidade do sistema jurídico quanto à sua capacidade de dar uma solução a um conflito de maneira rápida.

Por fim, o último elemento caracterizador do Direito Eletrônico, para fins dos nossos estudos, diz respeito a sua autorregulamentação, ou seja, o deslocamento do eixo legislativo para os participantes e interessados diretos na proteção de determinado direito e na solução de determinada controvérsia. Ou seja, os próprios participantes criam regras visando soluções práticas e dinâmicas (PINHEIRO, 2013, p. 82).

O Direito Eletrônico cria uma via paralela que não a via legislativa para criar regras de conduta para a sociedade digital. A autorregulamentação parte do pressuposto de que ninguém melhor que o próprio interessado para saber quais as lacunas que o Direito deve proteger, quais as situações práticas do cotidiano que se encontram sem o amparo do sistema jurídico e quais os caminhos corretos para se alcançar uma solução rápida e efetiva.

Exemplificando

Dois bons exemplos de autorregulamentação são: 1) Os provedores de serviços de acesso à internet, que têm contribuído e criado normas-padrão a serem seguidas não apenas em nível local, mas principalmente, em nível global, no que tange às questões de privacidade e de crimes virtuais; 2) O Código de autorregulamentação para a prática de e-mail marketing, acessível pelo endereço eletrônico http://www.capem.org.br.

Portanto, o pilar que sustenta essa autorregulamentação é justamente o de legislar sem muita burocracia, observando a Constituição e as leis vigentes, de modo a adequar a realidade jurídica à realidade social, garantindo dinamismo e flexibilidade às normas aplicáveis ao mundo virtual.

Até o presente momento, verificamos os elementos fundamentais do Direito Eletrônico (PINHEIRO, 2013, p. 77), mas, como era de se esperar, não são os únicos. Podemos citar vários outros que estão intrinsecamente ligados à própria

arquitetura da rede mundial de computadores, por exemplo:

- Publicidade (ou notoriedade): este elemento está diretamente ligado à autorregulamentação. É cediço que em nosso ordenamento jurídico, não se pode alegar o desconhecimento da Lei, como escusa para seu não cumprimento. A partir do momento que os próprios participantes da rede criam suas próprias regras, é recomendável que se dê publicidade às mesmas, para que os usuários destinatários se inteirem sobre as regras do jogo.

- Generalidade: as normas que regem a relação entre os participantes da rede devem ser essencialmente genéricas, de modo a facilitar o processo de consolidação de uma regra. Normas muitos específicas são de difícil aplicação em um ambiente sem barreiras geográficas, como é a internet.

- Uniformidade: este elemento simboliza a padronização dos atos praticados por aqueles que detêm a arquitetura da rede. Como bem exemplifica Patrícia Peck, se a Justiça condenou um determinado site em razão de eventual desconformidade com alguma norma legal, os outros sites devem passar a agir em conformidade com essa mesma norma, de modo a evitar que todos os consumidores ingressem no Judiciário para fazer valer seus direitos, evitando-se, assim, a elitização da Justiça (PINHEIRO, 2013, p. 79).

- Durabilidade (ou Continuidade): esta característica decorre do aspecto generalista do Direito Eletrônico, as normas consideradas "gerais" tendem a ser mais duradouras, pois são menos engessadas, adaptando-se melhor ao dinamismo característico da rede.

Faça você mesmo

Acesse o *link* http://pensando.mj.gov.br/marcocivil/texto-em-debate/minuta/ e contribua com o debate acerca da regulamentação do Marco Civil da Internet, dando sua opinião com base naquilo que aprendeu!

Sem medo de errar

Retomamos a situação-problema apresentada no início desta seção: você foi contratado por uma empresa para desenvolver sua plataforma de comércio eletrônico. A empresa exigiu conformidade do site com as leis aplicáveis à internet. Primeiramente você deve considerar o seguinte questionamento: Quais elementos de um ato jurídico, como a compra de uma mercadoria, merecem especial atenção quando realizado por meio da internet?

Para responder essa pergunta você deverá considerar os elementos do ato jurídico apresentados ao longo desta seção, e que são pilares na construção do Direito Eletrônico.

Atenção

Lembre-se que os elementos estão intrinsecamente ligados à própria natureza da internet, que se caracteriza pela ausência de limitação geográfica, instantaneidade e evolução constante, sendo que o sistema legislativo é incapaz de acompanhar as referidas mudanças.

Em resposta ao questionamento acima, os elementos de um ato jurídico que merecem especial atenção quando realizados pela internet são o local do ato (territorialidade), tempo em que o ato foi realizado e quais as normas que regulam aquele ato (regulação). Tais elementos formam a base do Direito Eletrônico.

Assim, você como desenvolvedor da plataforma deve garantir o registro de dados capazes de identificar onde e quando o ato foi praticado, bem como se a plataforma se apresenta em conformidade com as normas brasileiras e com as melhores práticas de mercados, ou seja, as normas delimitadas pelos próprios participantes da rede.

Avançando na prática

Regulando banco de dados de usuários?

Descrição da situação-problema

Você, renomado consultor na área de Tecnologia da Informação, foi contratado por um Deputado Federal para emitir um parecer, dando sua opinião sobre a possibilidade de criação de regras para regulação de sites de comércio eletrônico. A intenção do referido Deputado é criar uma lei determinando que os dados dos usuários que realizarem compras via internet devem ser armazenados em banco de dados desenvolvidos sob uma linguagem de programação específica e predeterminada pelo Ministério da Ciência e Tecnologia, de modo a facilitar a busca uniformizada por dados de contribuintes pelos órgãos vinculados ao Fisco. Sem considerar a legitimidade da demanda, que possivelmente fere o direito de privacidade dos usuários, responda o seguinte: É viável, ou mesmo desejável, estabelecer um padrão de programação pela via legislativa?

Lembre-se

Para responder ao questionamento acima, lembre-se que o sistema legislativo brasileiro caracteriza-se pela sua morosidade e ainda, que a tecnologia está em constante evolução.

Resolução da situação-problema

Conforme vimos ao longo desta seção, o Direito Eletrônico cria uma via paralela que não a via legislativa para criar regras de conduta para a sociedade digital. Esta autorregulamentação parte do pressuposto de que ninguém melhor que o próprio interessado para saber quais as lacunas que o Direito deve proteger, quais as situações práticas do cotidiano que se encontram sem o amparo do sistema jurídico e quais os caminhos corretos para se alcançar uma solução rápida e efetiva. Assim, não se apresenta viável, ou sequer desejável, a criação de uma lei visando o uso de determinada linguagem de programação para desenvolvimento de banco de dados. Tal ação engessaria o próprio mercado, que se prejudicaria em razão da morosidade do sistema legislativo.

Faça você mesmo

A partir do que estudamos nessa seção, você está habilitado para responder outras questões que levem em consideração os fundamentos do Direito Eletrônico e o funcionamento da internet. Convido você, aluno, a responder aos seguintes questionamentos: você considera a via judiciária como adequada para resolver os conflitos originados no meio virtual? Quais as vantagens das soluções não judiciais, como a arbitragem, muito usada em disputas envolvendo nomes de domínio?

Faça valer a pena

1. Considere as assertivas abaixo, julgando-as como corretas ou incorretas:

I. A origem da internet remonta desde a década de 1960, quando o Departamento de Defesa dos Estados Unidos da América fazia uso de uma rede conectada que utilizava tecnologia de comutação por pacotes de dados.

II. O protocolo NCP (Network Control Protocol), apresentava menor perda de pacotes durante a transmissão de dados, se comparado ao protocolo TCP/IP.

III. A internet foi exclusivamente responsável pelo fenômeno da globalização, tendo em vista seu poder de encurtar distâncias geográficas, aliado à troca quase instantânea de informações.

É correto aquilo que se afirma em:

a) I, apenas.

b) III, apenas.

c) I e II, apenas.

d) II e III, apenas.

e) I, II e III.

2. O Direito Eletrônico surgiu como alternativa ao "Direito Tradicional", como forma de resolver novos conflitos originados a partir do uso da rede por cada vez mais pessoas. Sobre o Direito Eletrônico, é incorreto afirmar que:

a) As primeiras discussões envolvendo o Direito Eletrônico sequer versaram sobre os problemas relacionados aos conflitos de jurisdição no espaço virtual.

b) O termo "Direito Eletrônico" pode ser considerado um sinônimo de "Direito Digital" e "Direito Virtual".

c) O Direito Eletrônico é marcado notadamente pela necessidade de seu operador possuir conhecimentos técnicos sobre conceitos computacionais e sobre a própria estrutura da rede mundial de computadores.

d) Segundo o filósofo Pierre Levy, o processo de virtualização não implica na perda da realidade, mas sim na mudança de seu eixo de gravidade.

e) Em razão da possibilidade de pessoas acessarem websites localizados em outros países e praticarem atos jurídicos, tais como jogos em cassinos, fora de seus países de origem, o problema da jurisdição foi o mais estudado na década de 1990.

3. Considerando o fenômeno da "desterritorialização", é correto afirmar que:

a) Uma vez que o Direito não é essencialmente territorial, pouca importância foi dada ao estudo da territorialidade no espaço virtual.

b) A aplicação do Direito aos atos e fatos jurídicos aperfeiçoados em meio virtual jamais mereceu especial destaque ou foi digno de discussão.

c) O Direito interno normalmente extrapola os limites geográficos do território de determinado Estado.

d) A extraterritorialidade da aplicação da lei é exceção à regra geral da territorialidade do Direito.

e) Os tribunais de um país geralmente enxergam com bons olhos, ou positivamente, o julgamento de seus cidadãos por tribunais estrangeiros.

Seção 1.2

Regulação do ciberespaço e a neutralidade da rede

Diálogo aberto

Na seção anterior estudamos as origens da internet e, consequentemente, do próprio Direito Eletrônico, analisando ainda seus principais elementos e características, no caso sua extraterritorialidade, dinamismo e regulamentação eminentemente feita pelos principais participantes da internet, como usuários e provedores. Nesta seção, iremos abordar a necessidade (ou não) de regulação do espaço virtual, ou ciberespaço e, consequentemente, qual o papel dos provedores na evolução da rede mundial de computadores e qual o limite desta atuação, ao passo que enfrentemos a questão da Neutralidade da Rede, muito debatida à época da aprovação da Lei nº 12.965 de 2014, conhecida como "Marco Civil da Internet".

Para tanto, devemos primeiramente retomar a solução geradora de aprendizagem (SGA) desta primeira unidade, qual seja: Suponhamos que você foi contratado por uma empresa do ramo de cosméticos para construir toda sua plataforma de e-commerce onde irá vender seus produtos aos seus consumidores. A empresa pediu que o site fosse construído em conformidade com as leis que regulam a internet e o comércio eletrônico, e ainda, que também restasse garantida a segurança das transações e veracidade dos dados do consumidor. Diante desse cenário, pergunta-se: Quais leis se aplicam à internet? É necessária a criação de leis específicas para regulação do espaço virtual? Como garantir a veracidade das informações prestadas pelo consumidor? Como criar rotinas sistêmicas capazes de preservar dados que poderão ser usados pela empresa em caso de ações na justiça?

Nesta seção, abordaremos uma situação-problema derivada da SGA acima apresentada. Nossa situação-problema utilizará os conceitos estudados na seção anterior, porém aprofundando-os, de modo a termos uma visão mais "macro" no tocante à criação de leis próprias para a internet. Nossa situação-problema para esta seção será a seguinte: O Diretor Comercial da empresa de cosméticos que o contratou quer saber se existem leis específicas para a internet, e ainda, como é feita a regulação do espaço virtual. Para resolver o problema exposto devemos aprofundar nossos estudos referentes ao conceito do Direito Eletrônico, sua abrangência, e a necessidade (ou não) de se criarem leis específicas para o meio digital, e ainda, qual o papel dos usuários e provedores na criação dessas eventuais leis.

Não pode faltar

Como você já deve ter percebido, a proposta deste curso não se limita a tratar somente do "direito aplicado à rede". Ao longo do curso, iremos abordar as principais implicações do direito no ambiente eletrônico. Assim, nossos estudos não se restringem ao "Direito da Internet", mas tratam também do "Direito Eletrônico", de modo a abranger situações diversas, como contratos eletrônicos, uso e assinaturas digitais, responsabilidade civil de provedores, crimes eletrônicos, além de várias outras situações.

A presença da tecnologia da informação nas várias situações do cotidiano demarca uma característica muito interessante do Direito Eletrônico, sua "multidisciplinaridade", ou seja, a influência dos diversos outros ramos jurídicos na formação deste ramo "especial". A título de exemplo, citamos abaixo alguns ramos do Direito e sua relação com o Direito Eletrônico:

- Direito Civil: O estudo da responsabilidade civil por atos ilícitos praticados pelo meio eletrônico é um exemplo da relação entre os dois ramos;
- Direito Penal: A criminalização de algumas condutas praticadas pelo meio eletrônico, como o acesso não autorizado a dispositivo informático (Art. 124-A do Código Penal) tem relação direta com o Direito Eletrônico;
- 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;
- Direito Constitucional: O eterno embate entre o Direito à Privacidade e o Direito à liberdade de expressão é objeto de estudo deste curso e retrata muito bem a importância de direitos constitucionais no Direito Eletrônico.

Estes são só alguns exemplos de relação dos diversos ramos do Direito com o Direito Eletrônico.

Assimile

A ciência jurídica ou o "Direito" é única, sua divisão entre diferentes ramos, como Direito Civil, Penal, Tributário, Trabalhista, é meramente doutrinária, de modo a facilitar seu estudo. Assim, o ramo do "Direito Eletrônico" busca analisar as implicações dos diversos ramos do direito no ambiente eletrônico.

A esta altura, você deve estar se perguntando o seguinte: Se o Direito Eletrônico se caracteriza por esta "mistura" de diversos outros ramos do direito, ele pode ser considerado como ramo autônomo do Direito?

Conforme nos ensina o Prof. Carlos Alberto Rohrmann, a questão da análise da autonomia de determinado ramo do direito passa pela busca de princípios próprios, que informem o pretenso ramo autônomo. Outros parâmetros que são utilizados na busca da demonstração da autonomia podem ser um corpo legislativo próprio, 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, p. 39).

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 uma área ou ramo específico do Direito? Ou seria simplesmente mero "reflexo" da tecnologia da informação nos ramos mais tradicionais, como Civil, Tributário, Trabalhista etc.?

Outro conceito interessante, relacionado diretamente à especialidade ou especificidade do Direito Eletrônico, refere-se justamente à "excepcionalidade da internet". Este conceito, inicialmente concebido pelo professor norte-americano Eric Goldman (2008), 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"? Qual os perigos de regulá-la da mesma maneira que regulamos outros setores, como a telefonia?

A discussão acerca da regulação da internet coincide também com a própria origem do Direito Eletrônico. Os primeiros estudos sobre o tema abordaram a necessidade (ou não) de um direito próprio para a rede, separado e diferente do chamado direito "tradicional". Ou seja, precisamos ou não de leis específicas para internet? Vários doutrinadores se propuseram a responder tal questionamento. A partir daí criaram-se as diferentes "correntes" sobre a regulação do ciberespaço (ROHRMANN, 2005, p. 13).

A primeira, chamada de "corrente libertária", foi a pioneira na publicação de artigos contundentes sobre a regulação do ciberespaço. Doutrinadores como Barlow, Post e Johnson ganharam projeção com artigos que questionavam a eficácia do direito tradicional para regulamentar os ambientes eletrônicos. Definitivamente o documento mais emblemático e que sintetiza os pensamentos dessa corrente é a "Declaração de Independência do Ciberespaço", publicada em 8 de fevereiro de 1996 e assinada justamente por John Perry Barlow, também fundador da ONG Eletronic Frontier Foundation (www.eff.org).

Pesquise mais

Indicamos a leitura do inteiro teor da "Declaração de Independência do Ciberespaço", que pode ser acessada no endereço eletrônico https://www.eff.org/cyberspace-independence. Neste documento, Barlow define o Espaço Virtual como um "mundo à parte", alheio e indiferente ao direito tradicional.

Podemos resumir a teoria libertária 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).

A crítica que se faz e esta corrente reside justamente no fato desta ver e definir o espaço virtual como um local separado do mundo real, como um lugar próprio, fora dos estados nacionais. Não se pode crer no surgimento de um Estado separado do mundo físico apenas porque se criou um ambiente de comunicação como a internet, que interliga vários Estados diferentes (ROHRMANN, 2005, p. 21). Você acredita que esta corrente teria aplicação prática no Brasil?

A segunda corrente, intitulada de "escola da arquitetura da rede", que encontra o professor Lawrence Lessig como seu principal expoente, se apoia na ideia da necessidade do 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-se que alguém do mercado determine um controle maior sobre a rede, pelo tipo de programação, de forma alheia à vontade do Estado. Esta corrente aponta as dificuldades de regulamentação jurídica do espaço virtual em face de algumas características técnicas do ambiente eletrônico, as quais vimos na Seção 1.1, como ausência de limites territoriais e o dinamismo da rede.

Lessig (1999) defende a tese de que ao espaço virtual não tem "natureza predefinida". O que irá determinar essa natureza é o "código" (*code*), que não se confunde com os códigos legais como o Código Civil ou o Código Penal, mas sim o código dos programas de computador que criam e moldam a forma de interação das pessoas na rede. Ele ainda alerta que a determinação da arquitetura da rede, ou seja, a condução da programação da internet, não poderia ser deixada a cargo exclusivo dos entes privados, nos casos os provedores de internet. 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.

Exemplificando

Um exemplo de aplicação das ideias da "escola da arquitetura da rede" diz respeito à utilização de programas de computador para filtragem do conteúdo da internet. O uso de programas de filtragem, inicialmente desenhados para pais preocupados em evitar o acesso de seus filhos a sites de pornografia, passou a ser adotado por empresas e até governos ao disponibilizarem acesso à rede. Trata-se justamente do Estado dizendo aquilo que é "impróprio" aos seus cidadãos e estabelecendo, por meio de código de programação, aquilo que pode ser acessado, ou não, na rede.

As críticas para essa corrente referem-se à possibilidade desta não considerar o direito como a melhor forma de solução de conflitos, elaborada para o bem comum e oriunda de um poder estatal, detentor do monopólio da força. Assim, pode-se dizer, embora não admitido pelos doutrinadores desta corrente, que esta traz em seu bojo a utopia de um espaço virtual, onde as "pessoas vivem" em relativa harmonia. Podemos entender tal ideal como utópico, tendo em vista, principalmente, a proliferação do discurso do ódio nas redes sociais.

A terceira corrente, chamada de corrente do "Direito Internacional", enxerga o espaço virtual como um "ambiente 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 esta corrente, o espaço virtual deve 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. Tal corrente sofreu críticas devido a sua difícil aplicabilidade prática, pois certos atos são melhor regulados por normas de direito interno, sobretudo aquelas referentes a atos privados, como contratos.

Por fim, temos a "corrente tradicionalista". Relembre que as duas correntes anteriores surgiram em razão das dificuldades de aplicação do direito tradicional ao ambiente eletrônico. A corrente tradicionalista não nega tais dificuldades, mas seu fundamento reside no entendimento de que o "direito" é muito mais amplo do que a simples possibilidade de aplicação da norma em uma situação concreta e específica. O direito tem algumas características próprias que o distinguem de outros sistemas de regras. Neste caso, as mais importantes são: a busca da justiça e do bem comum; a autoridade universal do direito e sua aplicação pelo ente público, o Estado. Desta maneira, esta corrente prega que o espaço virtual não é um local separado do mundo físico, como pensam os libertários, e também que regras baseadas no código de programação não é suficiente para coibir determinadas condutas, por exemplo, o acesso a conteúdos de pornografia infantil. Os mesmos criadores dos "códigos"

detêm a habilidade para contorná-los.

Esta corrente propõe a aplicação do Direito aos fatos jurídicos que ocorrem no espaço virtual. Desta maneira o ciberespaço poderia ser regulamentado sem maiores preocupações. A crítica a esta corrente reside justamente no fato de que os operadores do direito, em sua maioria, não possuem conhecimentos técnicos suficientes para aplicar o direito de maneira correta a situações ocorridas no espaço eletrônico, e ainda que os legisladores, muitas vezes, atuam em prol de interesses privados e, nem sempre, visando o bem comum.

Reflita

Apresentada as principais correntes do Direito Eletrônico e regulação do espaço virtual, qual dessas você considera a mais adequada?

Admitindo o caráter utópico da corrente libertária, entendemos que o ciberespaço é passível de regulação. A grande questão é a seguinte: como equacionar os diferentes interesses envolvidos na regulação da rede, especialmente Estado x Usuários x Provedores.

Esse embate quanto à regulação da internet teve seu mais recente exemplo nas discussões envolvendo a chamada "Neutralidade da rede". De maneira sintética, podemos definir a neutralidade da rede como um princípio que determina a obrigação dos provedores de acesso à internet de tratarem os pacotes de dados trafegados de maneira isonômica, ou seja, sem discriminar seu conteúdo ou origem. Como sabemos, o legislador brasileiro adotou o princípio da neutralidade da rede como uma obrigação legal, consubstanciada no artigo 9º da Lei nº 12.965, de 2014 ("Marco Civil da Internet").

Mas, qual é o impacto efetivo da referida regulação? Para os provedores de acesso significa a redução de eventuais lucros e, teoricamente, na diminuição de incentivos para melhorias na arquitetura da rede. Tais provedores alegam que estão sendo privados de lucrar com a venda de tráfego privilegiado para determinados provedores de conteúdo. Estes provedores de conteúdo, por sua vez, são beneficiados, pois há diminuição de barreiras para entrar no mercado. Assim, por exemplo, a "Netflix" não poderia comprar um tráfego privilegiado, o que abre o mercado para outros concorrentes que utilizam tecnologia de *streaming* de vídeos. Isso beneficiaria também os usuários, que teriam mais liberdade e autonomia para acessar conteúdos diversificados.

Atualmente, a neutralidade da rede no Brasil está pendente de regulamentação, cujo principal objetivo é reduzir os efeitos negativos que a neutralidade da rede impõe para os atores da internet no Brasil, ao mesmo tempo em que preserva suas características positivas. A fim de elucidarmos melhor a questão da neutralidade

da rede, principalmente seu aspecto prático, o que acha de retomarmos o cenário proposto em nossa SGA?

Perceba que a neutralidade impacta diretamente no setor de comércio eletrônico, ao passo que influencia o possível surgimento de novas empresas. A isonomia entre provedores garante a ampla concorrência, favorecendo o pequeno empresário. A ampla concorrência corrobora para a inovação e surgimento de novas tecnologias!

Pesquise mais

O assunto da Neutralidade da Rede é tratado de maneira bem didática pelo professor Pedro Ramos em seu site http://www.neutralidadedarede.com.br/. Pesquise mais o conteúdo e saiba as principais formas de discriminação de um conteúdo na internet.

Sem medo de errar

Vamos retomar nossa situação-problema, apresentada no início da seção: O Diretor Comercial da empresa de cosméticos que o contratou quer saber se existem leis específicas para a internet, e ainda, como é feita a regulação do espaço virtual. Para resolver o problema exposto devemos aprofundar nossos estudos referentes ao conceito do Direito Eletrônico, sua abrangência, e a necessidade (ou não) de se criarem leis específicas para o meio digital, e ainda, qual o papel dos usuários e provedores na criação dessas eventuais leis.

Atenção

Para resolver este problema você deve ficar atento aos pontos fortes e fracos das correntes do Direito Eletrônico que estudamos, bem como relembrar as características próprias do Direito Eletrônico e da internet.

As discussões acerca da regulação do ciberespaço remontam à época de surgimento do próprio Direito Eletrônico. Os doutrinadores da década de 1990 debatiam entre si qual a melhor forma de aplicação do Direito às situações jurídicas surgidas no meio eletrônico, ou ainda, se a aplicação do direito "tradicional" é sequer desejável, tendo em vista as peculiaridades da rede mundial de computadores, tais como a rápida e dinâmica troca de informações e a ausência de limites geográficos. A partir dessa divergência doutrinária surgiram quatro correntes diferentes que procuravam apresentar a possibilidade ou não de se aplicar o direito "tradicional" ao ciberespaço e como se daria tal aplicação.

A corrente "libertária" afirma não ser possível, nem desejável a regulação do espaço virtual, tendo em vista as características da internet. Nega-se a autoridade do Estado no ambiente eletrônico, que por sua vez encontra-se "desprovido de territorialidade" e dotado de uma "soberania própria". A corrente da "escola da arquitetura da rede" defende que o Estado deve intervir tão somente na criação do "código", ou seja, na criação da arquitetura da programação da rede, tendo em vista que os provedores e grandes empresas criariam as "regras" da internet, ou seja, aquilo que o usuário pode ou não fazer, de acordo com seus próprios interesses. A corrente do Direito Internacional, defende a aplicação de normas de Direito Internacional para regulação do ciberespaço. Por fim, a corrente "tradicionalista" afirma que as outras duas correntes possuem caráter utópico e somente através do Direito e o monopólio coercitivo do Estado é que os conflitos oriundos do espaço virtual poderiam ser resolvidos de forma satisfatória.

Posto isso, temos que, de acordo com a corrente libertária, não é possível a regulação do ciberespaço. Doutro lado, as correntes da escola da arquitetura da rede e a tradicionalista afirmar ser tal regulação possível, porém a primeira defende que essa regulação seja feita por meio do "código de programação" enquanto a segunda defende que a regulação deve ser feita por meio das "leis tradicionais". Apoiando-se nesta última o legislador brasileiro inovou em criar uma "lei tradicional" aplicável à internet. Trata-se justamente do Marco Civil da Internet!

Avançando na prática

Neutralidade da rede

Descrição da situação-problema

Você foi contratado por um startup multinacional, que deseja oferecer seus serviços de streaming de vídeo no Brasil, para exercer a função de gerente da área de TI. Essa empresa possui táticas "agressivas de mercado", sendo que em seu país de origem, ela remunera provedores de conexão para privilegiarem seu conteúdo em detrimento de seus concorrentes. O presidente da startup pretende reproduzir tal estratégia no mercado brasileiro e, para tanto, lhe consultou acerca da possibilidade de contratação de pacotes privilegiados junto a provedores de acesso. Responda: Tal estratégia é possível de ser reproduzida no Brasil, tendo em vista o disposto no artigo 9º da Lei nº 12.965/2014 ("Marco Civil da Internet")?

Lembre-se

A neutralidade da rede pode ser definida como um princípio que determina a obrigação dos provedores de acesso à internet de tratarem os pacotes de dados trafegados de maneira isonômica, ou seja, sem discriminar seu conteúdo ou origem.

Resolução da situação-problema

Como vimos anteriormente, o legislador brasileiro adotou o princípio da neutralidade da rede como uma obrigação legal, consubstanciada no artigo 9º da Lei nº 12.965 de 2014. Dessa maneira, os provedores de acesso à internet têm a obrigação de tratarem os pacotes de dados trafegados de maneira isonômica, ou seja, sem discriminar seu conteúdo ou origem. Assim, qualquer estratégia comercial no sentido de comprar um tráfego privilegiado de dados será considerada ilegal em território brasileiro.

Faça você mesmo

A neutralidade da rede gera grande discussões ao redor do mundo. Sua regulamentação não é fácil. Acesse o site http://pensando.mj.gov.br/marcocivil/texto-em-debate/minuta/ e conheça a minuta do decreto que pretende regulamentar o Marco Civil, sobretudo quanto à Neutralidade da Rede.

Faça valer a pena

1. Considerando o caráter multidisciplinar do Direito Eletrônico, indique qual das alternativas abaixo é a correta:

a) A criminalização de algumas condutas praticadas pelo meio eletrônico, como o acesso não autorizado a dispositivo informático (Art. 124-A do Código Penal) é um exemplo de interseção entre Direito Eletrônico e Direito Civil.

b) A questão da produção de prova a partir do meio eletrônico e sua validade jurídica é um exemplo de interseção entre Direito Eletrônico e Direito Ambiental.

c) O eterno embate entre o Direito à Privacidade e o Direito à liberdade de expressão é um exemplo de interseção entre Direito Eletrônico e Direito Constitucional.

d) O estudo da responsabilidade civil por atos ilícitos praticados pelo meio eletrônico é um exemplo da relação entre o Direito Eletrônico e o Direito Penal.

e) O Direito Eletrônico não possui nenhuma relação com os outros ramos do Direito.

2. Segundo o professor Carlos Alberto Rohrmann, são parâmetros para definir um ramo do direito como autônomo, exceto:

a) Princípios próprios.

b) Corpo legislativo próprio.

c) Estudo do ramo em cursos de graduação e pós-graduação.

d) Surgimento de profissionais especialistas na matéria.

e) Jurisprudência específica sobre a matéria.

3. O surgimento da internet marcou também as primeiras discussões acerca da aplicabilidade do Direito ao ciberespaço e sua consequente regulação pelo Estado. Desta maneira, surgiram diferentes correntes entre os doutrinadores do Direito Eletrônico, discutindo tal aplicabilidade. São correntes do Direito Eletrônico, exceto:

a) Corrente tradicionalista.

b) Corrente libertária.

c) Corrente da neutralidade da rede.

d) Corrente da "escola da arquitetura da rede".

e) Corrente do Direito Internacional.

Seção 1.3

Provas no meio digital

Diálogo aberto

Ao longo dos nossos estudos nesta Unidade, vimos os motivos que ensejaram os primeiros estudos sobre a aplicação do Direito às novas situações e problemas gerados a partir do uso constante da internet. Igualmente, analisamos os princípios do Direito Eletrônico e as diferentes correntes acerca da regulação do ciberespaço. Nesta seção, iremos estudar os procedimentos e regras aplicáveis à coleta segura e legal de provas produzidas no meio eletrônico, essencialmente o fenômeno da desmaterialização dos documentos físicos e a confiabilidade e segurança jurídica de documentos natos digitais.

Todavia, antes vamos retomar nossa situação geradora de aprendizagem (SGA)? Suponhamos que você foi contratado por uma empresa do ramo de cosméticos para construir toda sua plataforma de e-commerce onde irá vender seus produtos aos seus consumidores. A empresa pediu que o site fosse construído em conformidade com as leis que regulam a internet e o comércio eletrônico, e ainda, que também restasse garantida a segurança das transações e veracidade dos dados do consumidor. Diante desse cenário, pergunta-se: Quais leis se aplicam à internet? É necessária a criação de leis específicas para regulação do espaço virtual? Como garantir a veracidade das informações prestadas pelo consumidor? Como criar rotinas sistêmicas capazes de preservar dados que poderão ser usados pela empresa em caso de ações na justiça?

A partir de SGA acima, propomos a seguinte situação-problema: Ao desenvolver a plataforma de e-commerce do site de compras do seu cliente, o diretor jurídico da empresa pediu que, em caso de problemas ou inconsistências na compra de produtos por usuário, fossem preservadas eventuais provas que demonstrassem a regularidade da compra em eventual medida judicial proposta pelo usuário insatisfeito. Quais informações deverão ser guardadas?

Para resolver esse problema, devemos analisar o conceito de documento eletrônico, a legislação aplicável, bem como a admissibilidade do documento eletrônico em nosso ordenamento jurídico. Iremos estudar ainda os instrumentos probatórios mais utilizados quando o assunto são provas no meio digital.

Não pode faltar

Como sabemos, à medida que aparecem novas tecnologias e o meio eletrônico torna-se o principal meio para realização de negócios que possuem relevância jurídica, nos perguntamos como o direito irá conseguir acompanhar tal evolução. Tal questionamento foi debatido na Seção 1.1, quando analisamos os principais elementos do Direito Eletrônico. É justamente nesse cenário que surge a questão da possibilidade de utilização de um documento gerado no meio eletrônico como meio de prova em eventual processo judicial. Em um mundo cada vez mais "digitalizado", as ferramentas eletrônicas acabam servindo como meio de prova comum, por exemplo, a utilização de publicações nas redes sociais para comprovar a conduta dos usuários, ou sua opinião sobre algo ou alguém.

Passamos, portanto, por um período notadamente marcado pelo fenômeno da "desmaterialização" dos documentos. Ressalte-se que quando se trata de "desmaterialização" de um documento, não se quer indicar que não mais existe suporte físico para o documento, uma vez que o documento eletrônico fica inserido em um meio magnético. Diz-se "desmaterialização" indicando que não mais há a necessidade de um suporte físico para que o documento eletrônico possa ter sua validade. Isso porque o documento pode ao menos chegar a ser inserido em meio magnético, mas os dados podem ficar armazenados em um site ou em determinado programa na internet.

Mas o que é um documento? Em sentido amplo, um documento é toda e qualquer coisa que transmita diretamente um registro físico a respeito de algum fato, como os desenhos, as fotografias, as gravações sonoras, filmes cinematográficos etc. Já em sentido estrito, documento abrangeria somente os escritos, pois estes teriam a finalidade de registrar, através da palavra escrita, a existência de algum fato" (THEODORO JÚNIOR, 2001, p. 393).

Os documentos digitais se diferem dos documentos em papel, primeiramente, pela forma em que são registrados seus dados essenciais. Um documento digital é um arquivo de computador, somente compreensível por sistema de informação hábil a interpretar os comandos binários (I/0), ou seja, há a necessidade de um leitor, ao passo que um documento em papel normalmente já registra as informações no estado apto para cognição humana, apresar de depender que a pessoa já tenha sido alfabetizada ou tenha conhecimentos do idioma que tiver utilizado.

Assimile

Documentos são todos os registros de dados ou informações, independentemente do suporte onde tais registros são fixados!

Quanto ao suporte dos documentos, podemos dizer que este, para arquivos digitais, envolve o uso de mídias digitais, como disquetes, pen drives, discos ópticos, magnéticos, além da própria "nuvem" (armazenamento remoto permitido pela internet). Os documentos em meio físico são formalizados em papel, normalmente, mas também podem ser registrados em pedra, madeira, mineral, ou qualquer outro capaz de afixar informações.

Quanto à originalidade, documentos originais são todos aqueles em que é possível atestar os atributos de autenticidade de quem emite, e integridade do conteúdo ao longo do tempo. Um cheque assinado é documento original, pois pode passar por exame grafotécnico de quem assinou e de originalidade do papel utilizado, evitando-se, assim, eventuais fraudes. A digitalização de um cheque, sua microfilmagem ou reprografia são consideradas como cópias, visto que deixam de reunir todos os elementos que podem permitir a averiguação da autenticidade, devido à mudança de suporte, ainda que lei ou normativo específico confira efeitos legais idênticos ao de documento original.

Um e-mail é documento original em sua extensão nativa (.msg, .eml etc.), já a sua impressão em papel é mera cópia, uma vez que, em razão da migração de suporte, alguns atributos do documento digital, que são códigos hexadecimais combinados de 1 e 0 passam a não ser mais possíveis de serem observados, a exemplo de metadados ou função hash, sendo verificável apenas a interface gráfica, ou o texto da mensagem, não se podendo verificar nem mesmo a origem ou tráfego desta (dados de cabeçalho).

Vocabulário

Função *hash* é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo. Por esse motivo, as funções hash são conhecidas por resumirem o dado. A principal aplicação dessas funções é a comparação de dados grandes ou secretos. Dessa forma, as funções hash são largamente utilizadas para buscar elementos em bases de dados, verificar a integridade de arquivos baixados ou armazenar e transmitir senhas de usuários.

Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/07/o-que-e-hash.html>. Acesso em: 2 abr. 2016.

A cada dia testemunhamos a diminuição do receio da comunidade jurídica quanto à admissão de documentos eletrônicos como meios de prova em processo judicial. Isso se dá, principalmente, em razão de sua ampla utilização. Nesse passo, lecionam José Miguel G. Medina e Teresa Arruda A. Wambier: "Considera-se

documento qualquer representação material de um fato. Assim, filmes, fotografias, documentos eletrônicos, são cada um ao seu modo, documentos" (MEDINA; WAMBIER, 2009, p. 217).

Pesquise mais

Caso queira saber mais sobre documentos no formato digital indicamos a leitura do seguinte artigo: MARCACINI, Augusto Tavares Rosa. **O documento eletrônico como meio de prova**. Disponível em: <http://augustomarcacini.net/index.php/DireitoInformatica/DocumentoEletronico>. Acesso em: 01 jun. 2016.

Com efeito, a Lei nº 11.419/2006 ("Lei do Processo Eletrônico") torna o documento eletrônico admissível como meio de prova. A força probante deste tipo de documento passa a equivaler a de outros documentos tradicionais como o documento cartular (em papel) quando este apresentar determinados requisitos. O artigo 11 da citada Lei dispõe que os documentos produzidos eletronicamente e juntados aos autos de um processo judicial com garantias de origem e autoria são considerados originais para todos os efeitos legais. Cumpre ressaltar que a Lei nº 13.105, de 2015 ("Novo Código de Processo Civil") inovou ao prever expressamente a admissão e utilização de documentos eletrônicos em seu Capítulo XII "Das Provas" (artigos 439 a 441).

Uma vez definidos o conceito, validade e admissibilidade dos documentos eletrônicos, retomamos a nossa situação-problema: Quais as principais provas que podemos obter a partir de uma transação comercial eletrônica, e que poderão servir para instruir eventual ação judicial?

Para responder a tal questionamento, precisamos ter em mente que quanto mais elementos não manipuláveis no processo de guarda e armazenamento de provas forem envolvidos, maior a força do conjunto probatório, de modo a garantir a integridade e autenticidade daquele documento (eletrônico).

Assim, é recomendável que os provedores de aplicações, como é o caso da empresa descrita na SGA, guardem informações (registros eletrônicos) relativas ao: nome de usuário, data e hora com respectivo fuso horário, número de IP do usuário, além das mensagens trocadas entre empresa e usuário. Ou seja, todas as ações práticas pelo usuário de um site geram um log ou registro eletrônico. Quanto mais registros uma empresa tiver, maiores serão suas chances de êxito em eventual ação judicial.

Todavia, uma questão interessante surge: Considerando que o processo judicial eletrônico se encontra em fase inicial, sendo que a maioria esmagadora

dos processos no Brasil tramitam em autos físicos (em papel), como ficaria a questão dos documentos eletrônicos, uma vez que, como dito anteriormente, sua impressão, ou conversão em papel, retira sua originalidade e autenticidade?

Nestes casos, é comum as partes juntarem a cópia física do documento digital, sendo que sua originalidade ou autenticidade poderá ser discutida por meio de perícia técnica especializada. Ou seja, se uma das partes considerar que um e-mail juntado pela outra parte é falso, deverá ser realizada uma perícia técnica sobre aquele e-mail, analisando o cabeçalho original daquela mensagem, buscando os elementos que atestem sua originalidade.

Para evitar que um documento eletrônico seja questionado por perícia técnica, a parte pode valer-se, por exemplo, de uma Ata Notarial. A ata notarial é uma espécie de instrumento pelo qual o tabelião autentica algum fato, fazendo com que conste em seus livros; tendo a finalidade principal de tornar-se prova em processo judicial.

Vocabulário

Tabelião é um profissional do Direito, dotado de fé pública, a quem é delegado o exercício da atividade notarial, conforme prevê o artigo 3º da Lei nº 8.935/94, que dispõe sobre serviços notariais e de registro.

Ata notarial é a narração de fatos que o tabelião presenciou e transcreveu para um documento com fé pública e conteúdo probatório de uma escritura pública, o que lhe confere a situação de testemunha extrajudicial. O notário narra objetivamente os fatos, sem emitir juízo de valor. Assim, a ata evita o desaparecimento de um fato. Para os documentos eletrônicos, basta que se apresente seu conteúdo ao notário.

Exemplificando

Por exemplo, no caso de um site na internet, mostra-se ao tabelião o conteúdo disponibilizado na internet para que ele, a partir daquilo que vê e constata, redija a correspondente descrição em seus livros e lavre a respectiva ata notarial.

Assim, a ata notarial exerce a importante função de também declarar que as informações e fatos estão presentes e disponíveis para todos. Vale lembrar que, de acordo com o parágrafo único do artigo 193 do Novo Código de Processo Civil, são aplicáveis à prática de atos notariais, no que for compatível, as regras previstas em seus artigos 193 a 199, que disciplinam os atos processuais total ou parcialmente digitais, sistemas de automação que respeitem a publicidade dos atos etc. (TEIXEIRA, 2015, p. 158). Igualmente, o citado diploma processual

previu expressamente o uso da ata notarial como meio hábil para constar dados representados por imagem ou som gravados em arquivos eletrônicos (Art. 384).

Reflita

Diante do estudo, você acha que os chamados "prints" de tela, ou seja, a captura e impressão daquilo mostrado na tela de um computador em um determinado momento, possui valor probante? Qual a segurança jurídica desse documento?

Sem medo de errar

E agora, vamos resolver nossa situação-problema para esta seção: Ao desenvolver a plataforma de e-commerce do site de compras do seu cliente, o diretor jurídico da empresa pediu que, em caso de problemas ou inconsistências na compra de produtos por usuário, fossem preservadas eventuais provas que demonstrassem a regularidade da compra em eventual medida judicial proposta pelo usuário insatisfeito. Quais informações deverão ser guardadas?

Atenção

Os documentos digitais se diferem dos documentos em papel, primeiramente, pela forma em que são registrados seus dados essenciais. Um documento digital é um arquivo de computador, somente compreensível por sistema de informação hábil a interpretar os comandos binários (I/0).

Considerando que entre o usuário e a empresa cliente realiza-se verdadeira transação eletrônica, é natural que as informações advindas dos atos praticados pelas partes sejam produzidas também pelo meio eletrônico. Assim, quanto mais atividades do usuário forem registradas e armazenadas nos servidores da empresa, maior será a força do conjunto probatório. Assim, a empresa deverá armazenar os seguintes logs: nome de usuário, data e hora do ato praticado, número de IP do usuário, session ID, entre outros. Porém, devemos alertar o diretor jurídico que as impressões feitas a partir dos conteúdos desses documentos natos eletrônicos são meras reproduções e, se questionados judicialmente, deverá ser realizada perícia técnica informática nos arquivos originais. Outra opção é a lavratura de ata notarial por um Tabelião de Notas, capaz de atestar o conteúdo dos documentos eletrônicos.

Avançando na prática

Prevenção às fraudes eletrônicas

Descrição da situação-problema

O diretor do setor de segurança da informação da empresa de cosméticos verificou um grande aumento no número de fraudes eletrônicas praticadas na plataforma de comércio eletrônico da empresa. Vários usuários ingressaram com ações judiciais alegando cobrança indevida por parte da empresa, que vem sofrendo com a falsificação e uso indevido de dados de seus usuários por criminosos virtuais. Neste contexto, o citado diretor decidiu realizar uma reunião para verificar as possíveis soluções, de modo a ajudar o setor jurídico da empresa e, para tanto, pediu sua opinião sobre o caso. Quais informações devem ser armazenadas e qual sua importância?

Lembre-se

Quanto mais atividades do usuário forem registradas e armazenadas nos servidores da empresa, maior será a força do conjunto probatório em eventual demanda judicial.

Resolução da situação-problema

As principais informações que deverão ser armazenados são, principalmente, aquelas referentes a nome de usuário, data e hora do ato praticado, número de IP do usuário, session ID, entre outros. A importância dessa guarda reside justamente no fato de que cabe à empresa provar aquilo que alega em eventual procedimento judicial. Assim, é necessário estabelecer um conjunto probatório robusto, capaz de contradizer eventuais argumentos (falsos) utilizados pelo usuário.

Faça você mesmo

Sabendo que a originalidade e autenticidade de um documento eletrônico é aferida por meio da análise do arquivo digital original, abra uma mensagem de e-mail qualquer, acesse seu "original" (em linguagem de programação) e tente achar dentro do seu cabeçalho os metadados que poderiam servir para identificação de autoria desse documento eletrônico!

Faça valer a pena

1. São exemplos de documentos, exceto:

a) Fotografia.

b) Gravação sonora.

c) Filmagem.

d) Rumor.

e) Arquivo no formato .msg.

2. Sobre os documentos em formato digital, assinale a alternativa correta:

a) Trata-se de registro de informações em estado apto para imediata cognição humana.

b) É algo somente compreensível por sistema de informação hábil a interpretar os comandos binários (I/0).

c) Dispensa a necessidade de um leitor.

d) Não possuem o mesmo valor probante dentro de um processo judicial, se comparados aos documentos físicos.

e) Demandam uma perícia grafotécnica para apurar originalidade e autenticidade.

3. Indique a alternativa que contém um exemplo de suporte de documento físico:

a) Disquete.

b) Pen drive.

c) Disco rígido.

d) Disco óptico.

e) Papel.

Seção 1.4

Identidade digital e assinatura eletrônica

Diálogo aberto

Como você sabe, nesta unidade estudamos as origens do Direito Eletrônico e sua relação íntima com o próprio surgimento da internet, que por sua vez influenciou, de maneira demasiada, nos princípios e conceitos desse ramo do direito. Especificamente na última seção, analisamos o conceito de "documento" sob o viés jurídico, focando na legalidade dos documentos eletrônicos e suas peculiaridades técnicas e legais. Nesta seção, estudaremos o conceito de assinatura eletrônica e identidade digital, que estão intrinsecamente ligadas com nossos estudos sobre documento eletrônico, conforme iremos ver ao longo do nosso livro didático.

Porém, como é de praxe, vamos retomar nossa situação geradora de aprendizagem (SGA)? Suponhamos que você foi contratado por uma empresa do ramo de cosméticos para construir toda sua plataforma de e-commerce onde irá vender seus produtos aos seus consumidores. A empresa pediu que o site fosse construído em conformidade com as leis que regulam a internet e o comércio eletrônico, e ainda, que também restasse garantida a segurança das transações e veracidade dos dados do consumidor. Diante desse cenário, pergunta-se: Quais leis se aplicam à internet? É necessária a criação de leis específicas para regulação do espaço virtual? Como garantir a veracidade das informações prestadas pelo consumidor? Como criar rotinas sistêmicas capazes de preservar dados que poderão ser usados pela empresa em caso de ações na justiça?

A partir da SGA acima, propomos a seguinte situação-problema: Ao desenvolver a plataforma de e-commerce do site de compras do seu cliente (empresa do ramo de cosméticos), o diretor da área jurídica questionou a validade jurídica do uso de um "checkbox" como prova da aceitação dos Termos de Serviço do site pelo usuário, ou seja, para efetuar uma compra no site o usuário deve realizar um cadastro, inserindo seus dados pessoais e, ao final, aceitar os termos de uso do site clicando em um "checkbox". O aceite do usuário por meio de um clique num "checkbox" possui validade jurídica?

Para resolver esse problema, iremos analisar o conceito de assinatura identidade digital e assinatura eletrônica, com e sem certificação digital, os aspectos técnicos acerca do tema, bem como a legislação aplicável.

Não pode faltar

A popularização da internet no Brasil trouxe inúmeros benefícios e comodidades aos seus usuários, que passaram a realizar várias operações por meio dela, como a automatização de operações bancárias, a realização de compras de mercadorias a distância, o armazenamento de documentos e arquivos em formato digital na "nuvem", entre outros. Paralelamente aos benefícios, várias pessoas visualizaram nesses meios formas de obter ganhos ilicitamente, inclusive criando mecanismos para capturar dados pessoais como senhas, números de contas bancárias e cartões de crédito. Contudo, isso não foi motivo suficiente para as pessoas deixarem de usar a internet e realizar transações eletrônicas em seu cotidiano.

Tendo em vista o uso maciço da tecnologia da informação e a possibilidade de seu uso para fins fraudulentos, busca-se a todo momento criar ferramentas que possam dar segurança às relações estabelecidas pelo meio eletrônico. É preciso ter segurança quanto à identidade dos usuários que realizam transações e interagem entre si. Ou seja, é necessário sabermos se quem está por trás da tela do computador é quem realmente diz ser. Precisamos confirmar sua identidade digital.

Dentre essas ferramentas, desenvolveu-se um método pelo qual seria possível identificar a pessoa e garantir a integridade dos dados transmitidos. Estamos falando da assinatura eletrônica. Assinatura é toda marca, sinal ou operação que confira autenticidade à declaração de vontade e fixa seu teor, de forma íntegra no tempo e espaço pelo emissor, onde autenticidade é o atributo que atesta a identidade do declarante (a pessoa é ela mesma) e a integridade é o atributo que determina que o estado dos dados emitidos pelo declarante não foi alterado após a aposição de assinatura.

Assimile

"Assinar" um documento significa 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.

Assim, 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.

De acordo com o artigo 104 do Código Civil Brasileiro, os negócios jurídicos são válidos sempre que envolverem objeto lícito, possível, determinado ou determinável, agentes capazes e forma prescrita ou não defesa em lei. Nesse contexto, as contratações eletrônicas (ex.: compra e venda de mercadoria por meio de um website) nada mais são que negócios jurídicos firmados em meio eletrônico, portanto, submetidas a todos os requisitos de validade dispostos no referido artigo 104 do Código Civil.

A validade da assinatura eletrônica diz respeito diretamente à forma não defesa em lei (não proibida em Lei), uma vez que permitida sempre que a lei específica não diga o contrário, pois o Direito Brasileiro adotou a prática da forma livre como padrão.

Dentro do nosso ordenamento jurídico, no que tange ao uso de assinaturas eletrônicas, destacamos a Medida Provisória n. 2.200-2 de 2001, que em seu artigo 10º prescreve que as declarações de vontade ratificadas por assinaturas digitais apostas por meio de 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 do uso de outras formas de assinatura digital, desde que aceitas pelas partes envolvidas ou forem admitidas de tal forma.

Assinar digitalmente um documento significa executar uma função tecnológica que lhe confira marca específica e que seja impossível de ser dissociada sem alterar seu conteúdo – bytes que estão em linguagem hexadecimal, e não a mensagem que é exibida na tela. Todos os arquivos digitais possuem alguma espécie de assinatura nativa, por isso que os softwares mais recentes já conseguem indicar evidências de autenticidade nos documentos através de pequenos bytes que não alteram a visualização na tela (o que é vista na interface mais externa), mas marcam como o arquivo foi gerado ou até mesmo por quem!

Exemplificando

Os bytes acima citados podem ser alterados? Sim! Exceto se for executada uma função tecnológica de controle e bloqueio. Cite-se, por exemplo, os metadados de arquivos, que podem ser alterados acionando as propriedades com o botão direito do mouse.

São várias as formas de assinaturas eletrônicas, desde uma simples assinatura digitalizada até o uso de biometria. Em razão do fenômeno da "desmaterialização", que tratamos na Seção 1.3 desta Unidade, criou-se o sistema de assinatura digital, sendo que, a fim de conferir maior segurança jurídica a esse processo, tanto o mercado quanto as autoridades governamentais passaram a utilizar, de maneira ampla, a certificação digital de documentos, por meio da criptografia, com o fim de trazer mais segurança e minimizar chances de fraudes.

Vocabulário

A **criptografia** é um método matemático que cifra uma mensagem em código, ou seja, transforma-a em caracteres indecifráveis, podendo ser simétrica ou assimétrica.

Por razões de segurança, a criptografia assimétrica é a mais utilizada. Esta, por sua vez, cria um código e uma senha para decifrá-lo, isto é, conhecem-se duas chaves: uma chave privada, que codifica a mensagem, e outra pública, que decodifica a mensagem. Entretanto, o inverso pode ocorrer, ou seja, a pública codifica e a privada descodifica. O emissor da mensagem fica com a chave privada, e os destinatários de suas mensagens ficam com a chave pública. Esse sistema dá segurança aos negócios efetuados na internet, devendo ser controlado por uma terceira entidade, que é a autoridade certificadora, que atua como um "tabelião virtual", que irá conferir a autenticação digital das assinaturas e dos documentos. Diferentemente, a criptografia simétrica cria uma mesma chave tanto para criptografar, quanto para descriptografar (TEIXEIRA, 2015, p. 159).

Exemplificando

Atualmente, já estão disponíveis o e-CPF e o e-CNPJ. Estes certificados digitais são documento eletrônicos com fim de comprovação de identidade digital, emitidos por autoridade certificadora credenciada pela ICP-Brasil e habilitada pela Receita Federal Brasileira, que confere legitimidade dos emissores e destinatários dos documentos e dados que trafegam numa rede de comunicação, assegurando ainda privacidade e inviolabilidade.

Além da certificação digital, existem outras formas de assinaturas digitais, por exemplo, a combinação de nome de usuário e senha, amplamente utilizada e tida como segura pelas obrigações de confidencialidade e complexidade estabelecidas pelo agente autenticador (ex.: site de internet). Quando se adota um modelo de assinatura digital significa dizer que o processo de autenticação (verificação

do emissor da declaração ou autor do ato jurídico) envolve a coleta, criação e conferência de dados de forma informatizada, portanto, com apoio de recursos de computação.

A legislação brasileira recepcionou a mais ampla maneira de fixação de suporte para os documentos, conforme vimos na seção anterior, aceitando métodos físicos, mecânicos, eletrônicos e digitais como meio de prova, até que seja apresentada contraprova que possa demonstrar a falsidade ou outra forma de invalidade documental.

Como dito anteriormente, a lei não obsta o uso de outras formas de assinatura digital fora do padrão ICP-Brasil, desde que a declaração de vontade seja aceita pelas partes, as quais gerarão os efeitos pretendidos, conforme o já citado artigo 10º, da MP 2.200-2 de 2001. Isto significa que, na prática, nos Termos de Serviço do site ou aplicativo no qual se pretende utilizar assinatura digital baseada em nome de usuário e senha, deverá estar expressamente previsto o aceite das partes quanto à validade deste tipo de assinatura.

Porém, entendemos que a aceitação deste tipo de assinatura digital estar simplesmente prevista nos termos de serviços não é suficiente para que o titular do site ou aplicativo tenha segurança jurídica quanto ao processo de autenticação da identidade digital. É necessária ainda a manifestação expressa da vontade do usuário. Tal validação pode ser efetuada, por exemplo, por meio de um "checkbox", ou seja, a adesão do usuário aos termos de serviço é realizada através da marcação de um campo de aceite, no qual a parte afirma ter ciência e concorda com os termos daquela contratação.

A dificuldade prática que se apresenta quanto a esta modalidade de aceite refere-se à forma de comprovação dessa contratação caso o contrato venha a ser discutido judicialmente. Isso porque a aceitação do usuário deverá ser demonstrada mediante os registros eletrônicos de sua conta, os chamados logs de navegação. Lembrando que entre empresa e usuário existe verdadeira relação de consumo, aplicando as normas próprias do Código de Defesa do Consumidor, inclusive a chamada inversão do ônus da prova. Vale dizer que, em eventual discussão judicial, caso o usuário afirme que, em nenhum momento, aceitou os termos de uso, cabe à empresa a demonstração do fato, que poderá ser comprovado com a juntada dos logs de navegação, já discutidos na última seção, como número de IP, session ID, data e horas de acesso, geolocalização etc. Quanto mais registros de atividades, maior força possui o conjunto probatório.

Dessa maneira, o aceite mediante o preenchimento de checkbox é juridicamente válido, ao passo que demonstra ciência inequívoca do usuário quanto aos termos e condições que regem determinada contratação realizada pelo meio eletrônico.

Pesquise mais

Sobre o uso de assinaturas digitais com e sem certificação digital, para contratações eletrônicas recomendamos a leitura da seguinte obra: LUCCA, Newton de. **Aspectos Jurídicos da Contratação Informática e Telemática**. São Paulo: Saraiva, 2003.

Sem medo de errar

Passemos agora à resolução da nossa situação-problema:

Ao desenvolver a plataforma de e-commerce do site de compras do seu cliente (empresa do ramo de cosméticos), o diretor da área jurídica questionou a validade jurídica do uso de um "checkbox" como prova da aceitação dos Termos de Serviço do site pelo usuário, ou seja, para efetuar uma compra no site o usuário deve realizar um cadastro, inserindo seus dados pessoais e, ao final, aceitar os termos de uso do site clicando em um "checkbox". O aceite do usuário por meio de um clique num "checkbox" possui validade jurídica?

Atenção

A lei brasileira não obsta o uso de formas de assinatura digital fora do padrão ICP-Brasil, desde que a declaração de vontade seja aceita pelas partes, as quais gerarão os efeitos pretendidos, conforme o artigo 10º, da MP 2.200-2 de 2001.

A assinatura digital por meio de Login e senha de usuário possui validade jurídica em nosso ordenamento. Todavia, tal modalidade deve estar expressamente prevista nos Termos de Serviço do nosso site. Ocorre que o fato da aceitação deste tipo de assinatura digital estar simplesmente prevista nos termos de serviços não é suficiente para que a empresa (cliente) tenha segurança jurídica quanto ao processo de autenticação da identidade digital. É necessária ainda a manifestação expressa da vontade do usuário. Tal validação pode sim ser efetuada por meio de um "checkbox", ou seja, a adesão do usuário aos termos de serviço é realizada através da marcação de um campo de aceite, no qual a parte afirma ter ciência e concorda com os termos daquela contratação. A fim de dar maior segurança jurídica à contratação, a empresa deve ainda guardar em seus servidores a maior quantidade possível de registros de navegação do usuário, de modo a conferir maior força ao conjunto probatório em caso de ação judicial onde a adesão ao contrato de compra e venda é questionada.

Avançando na prática

Li e concordo com os termos de serviço do site

Descrição da situação-problema

Determinada empresa que deseja construir um site para realizar a venda de produtos para usuários cadastrados, como roupa, eletrônicos, acessórios etc. Tal empresa contratou-o para desenvolver a plataforma, sendo que uma necessidade específica é a celebração dos contratos com fornecedores pelo meio eletrônico. Tendo em vista tal situação, a empresa deseja saber se é obrigatório o uso de certificação digital para celebração dos referidos contratos.

Lembre-se

Dentro do nosso ordenamento jurídico, no que tange ao uso de assinaturas eletrônicas, destaca-se a Medida Provisória n. 2.200-2 de 2001, que em seu artigo 10º trata sobre o uso de assinaturas eletrônicas.

Resolução da situação-problema

Dentro do nosso ordenamento jurídico, no que tange ao uso de assinaturas eletrônicas, destacamos a Medida Provisória n. 2.200-2 de 2001, que em seu artigo 10º prescreve que as declarações de vontade ratificadas por assinaturas digitais apostas por meio de 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 do uso de outras formas de assinatura digital, desde que aceitas pelas partes envolvidas ou forem admitidas de tal forma.

Além da certificação digital, existem outras formas de assinaturas digitais, por exemplo, a combinação de nome de usuário e senha, amplamente utilizada e tida como segura pelas obrigações de confidencialidade e complexidade estabelecidas pelo agente autenticador (ex.: site de internet).

Destarte, o uso de certificação digital para celebração de contratos entre empresa e fornecedores, pelo meio eletrônico, não é obrigatório, podendo a empresa utilizar outras formas de assinatura eletrônica, como usuário/senha ou biometria. Todavia, é necessário que conste em tal contrato cláusula específica onde as partes conferem eficácia à contratação eletrônica.

Faça você mesmo

Sugerimos que você acesse seu site favorito e crie uma nova conta de usuário! Verifique qual o método de aceitação utilizado por este!

Faça valer a pena

1. Considere as afirmativas abaixo:

I – O uso maciço da tecnologia da informação aliada à possibilidade de seu uso para fins fraudulentos, ensejou a necessidade de criação de ferramentas que possam dar segurança às relações estabelecidas pelo meio eletrônico.

II – A confirmação da identidade digital de um usuário é dispensável durante o processo de autenticação de uma transação eletrônica.

III – O uso de mecanismos de assinatura eletrônica está diretamente ligado ao processo de confirmação da identidade digital do usuário.

Quais das afirmativas acima estão corretas?

a) I, apenas.

b) I e II.

c) II e III.

d) I e III.

e) III, apenas.

2. Complete o espaço em branco com o termo que melhor se enquadra à respectiva definição:

_____ é toda marca, sinal ou operação que confira autenticidade à declaração de vontade e fixa seu teor, de forma íntegra no tempo e espaço pelo emissor.

a) Identidade.

b) Biometria.

c) Assinatura.

d) Certificação.

e) Nenhuma das anteriores.

3. De acordo com o artigo 104 do Código Civil Brasileiro, são elementos que conferem validade aos negócios jurídicos, exceto:

a) Objeto lícito.

b) Objeto indeterminado.

c) Agentes capazes.

d) Forma prescrita em lei.

e) Forma não defesa em lei.

Referências

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

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

LÉVY, Pierre. **O que é virtual?** São Paulo: Ed. 34, 1996.

LUCCA, Newton de. **Aspectos jurídicos da contratação informática e telemática**. São Paulo: Saraiva, 2003.

MEDINA, José Miguel G.; WAMBIER, Teresa Arruda Alvim. **Processo civil moderno**. v. 1. São Paulo: RT, 2009.

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

ROHRMANN, Carlos Alberto. **Curso de direito virtual**. Belo Horizonte: Del Rey, 2005.

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

THEODORO JÚNIOR, Humberto. **Curso de direito processual**. v. 1, 36. ed. Rio de Janeiro: Forense, 2001.

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

Direitos fundamentais e responsabilidade civil

Convite ao estudo

Você sabia que as ofensas publicadas na Internet são puníveis, tanto em âmbito civil (indenizatório) quanto criminal? Ou então, que violar a privacidade de usuários é igualmente punível? Nesta unidade iremos estudar os chamados "direitos fundamentais" e suas particularidades quando exercidos na Internet. Iremos nos debruçar sobre o direito à honra, imagem, privacidade e liberdade de expressão, bem como a colisão entre tais direitos no ambiente eletrônico. Vimos na Unidade 1 o funcionamento básico da internet e os fundamentos do Direito Eletrônico. A partir daí, iremos perceber a importância do direito para a resolução de conflitos oriundos do ambiente on-line, tomando como referência a corrente tradicionalista do Direito Eletrônico.

Iremos conhecer os principais dispositivos legais aplicáveis à temática, com especial destaque para a Constituição Federal de 1988, o Código Civil Brasileiro, além do Marco Civil da Internet. O objetivo específico desta Unidade é justamente ensinar como resolver conflitos entre direitos fundamentais quando estes colidem em um ambiente virtual, e ainda, o dever de reparação por parte de usuários ou provedores em caso de comprovação de dano, próprio do instituto da responsabilidade civil, consagrado em nosso ordenamento jurídico.

Para a Unidade 2, partiremos da seguinte situação geradora de aprendizagem (SGA): Suponhamos que você foi contratado por uma empresa na qual a principal atividade é a produção de conteúdo para publicação no site Youtube. Tal empresa possui ainda um website que diariamente publica conteúdos relacionados à cultura pop, como cinema, quadrinhos, jogos etc. A empresa deseja desenvolver uma plataforma de rede social para que seus usuários interajam entre si e compartilhem conteúdos diversos. Seu trabalho consiste em desenvolver toda a infraestrutura dessa rede social, bem como realizar a blindagem jurídica da nova aplicação, ou seja, como minimizar os riscos de a empresa vir a ser punida judicialmente em razão de eventuais conteúdos ilícitos publicados pelos usuários. Para

solucionar esta questão, devemos refletir acerca da reponsabilidade dos provedores de aplicação por atos praticados por usuários. Até que ponto o provedor é responsável? Deve o provedor tomar alguma medida preventiva para mitigar eventuais prejuízos ou a Lei resguarda a empresa de maneira satisfatória?

Ao longo desta unidade iremos estudar o que são direitos fundamentais, qual sua importância para o desenvolvimento de uma internet livre e segura, como resolver eventuais conflitos e qual a responsabilidade civil dos usuários e dos provedores.

Seção 2.1

Direitos fundamentais na internet

Diálogo aberto

Conforme sabemos, a internet foi concebida como um ambiente livre e democrático, no qual o conteúdo é produzido e compartilhado por todos os seus usuários. Todavia, muitos desses conteúdos violam uma ou mais leis deste ou daquele país. A colocação em rede de conteúdos ilícitos pode desencadear ofensa a uma variada gama de direitos individuais. Como os conteúdos são diversos, também diversas são as categorias de direitos que por eles podem ser atingidas.

As principais questões práticas decorrentes da transmissão e publicação de informações na internet, no entanto, estão relacionadas com mensagens difamatórias ou que violem a privacidade de terceiros, suscetíveis de causar danos à reputação e imagem de uma pessoa. Além disso, é igualmente comum conteúdos que violem o direito à propriedade intelectual de terceiro, porém estes serão analisados na Unidade 3.

A internet tornou-se um campo fértil para a disseminação de conteúdos diversos, sendo um dos principais instrumentos para garantias de princípios democráticos, como a liberdade de expressão ou livre manifestação do pensamento. Mas, como proteger tais liberdade sem violar outros direitos igualmente importantes como a honra e privacidade?

Relembremos nossa situação-geradora de aprendizagem (SGA): Suponhamos que você foi contratado por uma empresa que possui um website, no qual, diariamente, são publicados conteúdos relacionados à cultura pop. A empresa deseja desenvolver uma plataforma de rede social para que seus usuários interajam entre si e compartilhem conteúdos diversos. Seu trabalho consiste também em realizar a blindagem jurídica desta nova aplicação, conforme explicado.

Para esta seção, iremos considerar a seguinte situação-problema: ao desenvolver a rede social, o dono da empresa pediu que você pontuasse e analisasse os principais direitos fundamentais dos usuários com os quais a empresa deve se preocupar ou dar mais atenção. Dentre os vários direitos fundamentais, quais são aqueles que, na prática, apresentam maior vulnerabilidade na internet? Para tanto

estudaremos os conceitos de direitos fundamentais e os principais diplomas legais que protegem tais direitos.

,

Não pode faltar

Atualmente é aceito, sem discussão, que uma das ideias básicas do mundo jurídico ocidental se refere aos direitos fundamentais. Na verdade, são os direitos fundamentais reconhecidos por um Estado a melhor via para se constatar seu caráter democrático ou não, liberal ou social. Além desse entendimento comum, existe também controvérsia sobre o alcance e grau de exigibilidade desses direitos, assim como sobre as transformações que ocorrem no sistema jurídico em consequência de sua positivação constitucional, ou seja, quando são transformados em dispositivos legais previstos na legislação, especificamente na Constituição.

Entretanto, existe um consenso acerca da necessidade de proteção desses direitos, não só no campo teórico, mas também na prática. É necessário dar efetividade a esses direitos. Após a popularização da internet e o advento das redes sociais e do comércio eletrônico, a necessidade de proteger tais direitos aumentou consideravelmente, tendo em vista o papel catalisador que o meio eletrônico exerce. A publicação de um conteúdo ofensivo é visualizada por milhares de pessoas em diferentes lugares; empresas como Facebook ou Google possuem um "mar" de dados pessoais de usuários. Preceitos como "honra", "privacidade" e "liberdade de expressão" nunca foram tão relevantes.

Como dissemos, existe uma consciência generalizada sobre a urgência da proteção efetiva dos direitos fundamentais. Mas, antes de protegê-los, é necessário que realizemos sua correta identificação. Ora, como proteger algo sem antes delimitá-lo?

Para essa identificação, podemos agrupar os caracteres diferenciadores em dois grupos básicos: o que os distingue segundo a posição formal que ocupam no ordenamento jurídico e o que os identifica consoante a matéria que regulam (CASTRO, 2002, p. 80).

Pelo critério formal de identificação, os direitos fundamentais seriam aqueles inseridos em instrumentos internacionais, tais como convênios, protocolos, constituições, tratados etc. (Exemplificando: A Declaração Universal dos Direitos Humanos é um documento internacional, ratificado por vários países, que define e protege diversos direitos fundamentais). Isso garante a estes direitos um regime jurídico diferenciado, ou seja, uma proteção "extra", derivada justamente de uma espécie de "hierarquia" ou status superior dentro de um ordenamento jurídico.

Esse critério, contudo, não é suficiente, pois dita sistematização pode suscitar

dúvidas, por exemplo, sobre se todos os direitos consagrados nas constituições no título próprio são fundamentais ou não. É o que ocorre quando se procura definir se a liberdade de imprensa, prevista no artigo 220 da Constituição Federal de 1988, é ou não um direito fundamental, uma vez que não consta no rol dos direitos elencados no art. 5º do referido diploma legal, que trata especificamente dos direitos fundamentais.

Doutro lado, se considerarmos a existência de um critério objetivo do ponto de vista material, os direitos fundamentais são, em geral, aquelas prerrogativas das pessoas, que são consideradas de maior importância na consciência e cultura jurídicas de determinada sociedade. Em outras palavras, é um direito fundamental, do ponto de vista material, se sua existência tem um grau de necessidade que, sem ele, não se poderia desenvolver determinada concepção do Estado e da sociedade.

Assim, importaria averiguar quais seriam os direitos que, em razão do entendimento social dominante em uma determinada época, podem ser tidos como imprescindíveis, conferindo assim o caráter "fundamental".

Apresentadas as duas teorias (formalista e materialista), qual delas é adotada no Brasil? Poderíamos dizer que o Brasil adota uma espécie de teoria "mista". Confuso? Então iremos explicar melhor. É necessário construirmos uma "doutrina" constitucional dos direitos fundamentais apoiada em uma constituição cujas normas estejam, de fato, escritas, e não apenas uma teoria de direitos fundamentais abstratos, ou seja, que fique somente no campo das ideias (CANOTILHO, 1988, p. 1249).

Assimile

Para sabermos se um direito possui o status de "fundamental" ou não, devemos avaliar tanto o seu aspecto formal (se está na Constituição) quanto seu aspecto material (se tal direito é, por exemplo, uma garantia democrática). Assim, conceituar um direito fundamental é uma tarefa complexa, mas nos arriscamos a dizer que fundamentais são todos os direitos que têm como principal finalidade proteger a dignidade humana em todas as dimensões.

Estabelecido um conceito de "direito fundamental", passaremos à análise da proteção dos direitos fundamentais dentro do ordenamento jurídico brasileiro. Vale esclarecer que cuidaremos de alguns direitos que podem entrar em rota de colisão, tendo em vista o advento da internet. Considerando o que foi até aqui estudado, sobretudo com relação às principais características e elementos do Direito Eletrônico, são vários os direitos fundamentais envolvidos, como a liberdade de expressão, a privacidade, o sigilo da correspondência, da comunicação e dos dados, o direito à honra e à imagem.

Alguns desses direitos também passaram a ser objeto de legislação específica, no caso, o Marco Civil da Internet (Lei nº 12.965/2014). Tal fato reitera o caráter "misto" no tocante à delimitação dos direitos fundamentais, pois determinado direito pode ser alçado ao nível de "fundamental" mesmo não constando na Constituição Federal.

Não obstante, a Constituição Federal, definitivamente, serve como bússola para delimitarmos o caráter "fundamental" de um direito. Isso se explica, em grande parte, em razão do fenômeno da "constitucionalização" dos direitos fundamentais, que pode ser explicada como a positivação (ou formalização) dos direitos fundamentais.

Ora, a Constituição é nossa norma suprema, vinculando os Poderes do Estado (Executivo, Legislativo e Judiciário) aos preceitos lá contidos. Assim, a sistematização dos direitos fundamentais na Constituição, particularmente em seu artigo 5º, os alçou à dimensão substancial do texto constitucional, ou seja, essenciais para o desenvolvimento de uma democracia.

Reflita

Por serem essenciais, podem os direitos fundamentais ser considerados absolutos, ou seja, irrestritos, incapazes de serem limitados? De acordo com a moderna doutrina, não existem direitos absolutos! Em caso de conflito, deverá ser analisado o caso concreto, conforme veremos nas próximas seções.

Além da Constituição Federal de 1988, outros diplomas legais protegem os direitos fundamentais de eventuais abusos e violações, inclusive no meio eletrônico. A título de exemplo, o Código Civil dedica um capítulo específico para os chamados "Direitos da Personalidade". Consideram-se da personalidade os direitos reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previstos no ordenamento jurídico exatamente para a defesa de valores inatos ao homem, como a vida, a intimidade, a honra e tantos outros (BITTAR, 2001).

Cumpre esclarecer que o conteúdo dos Direitos da Personalidade é essencialmente o mesmo se comparado aos direitos fundamentais, porém, com estes não se confundem. Os direitos fundamentais possuem um caráter "público", ou seja, protegem o indivíduo contra abusos praticados por parte do Estado, enquanto os direitos da personalidade protegem um indivíduo contra as ações de outro indivíduo, no âmbito das relações "privadas". Essa distinção possui caráter doutrinário, mas, na prática, o conteúdo é o mesmo.

A fim de demonstrar isso, elegemos três direitos fundamentais, previstos no artigo 5º da Constituição Federal de 1988, e que são também direitos da personalidade, previstos no Código Civil Brasileiro. São eles a honra, a privacidade e a liberdade. Tais direitos são os que constantemente entram em rota de colisão dentro de um ambiente on-line.

A exemplo disso, temos várias situações cotidianas em que esse "conflito" resta evidente, como a remoção de comentários ofensivos e difamantes das redes sociais, a recusa de provedores em fornecer determinados dados privados de modo a resguardar a liberdade de expressão de seus usuários, além de outros.

O reconhecimento do direito à honra prende-se à necessidade de defesa da reputação da pessoa (física ou jurídica), compreendendo o bom nome e a fama de que desfruta perante a coletividade, enfim, a estima que a cerca nos seus ambientes, familiar, profissional, comercial ou outro. Alcança também o sentimento pessoal de estima ou a consciência da própria dignidade.

A honra pode ser atingida pela falsa atribuição de crime ou pela imputação de fato ofensivo à reputação, com alteração da posição da pessoa na coletividade, entendendo-se suscetíveis de prejudicar pessoa física e pessoa jurídica.

Exemplificando

A título de exemplo, podemos citar um comentário publicado em um site de reclamações (ex.: www.reclameaqui.com.br). A depender do teor do comentário, ou seja, se nele constar algum fato inverídico ou que de alguma maneira viole a honra da empresa, tal publicação poderá ser removida.

O direito à privacidade, ou intimidade, refere-se ao direito que a pessoa tem de se resguardar contra injunções, indiscrições ou intromissões alheias. Esse direito vem assumindo, cada vez mais, maior protagonismo, sobretudo em razão da evolução das técnicas de comunicação. Como sabemos, o usuário da rede está cada dia mais exposto. Seus dados pessoais trafegam na rede de maneira indiscriminada, tendo valor financeiro relevante, haja vista os investimentos em marketing e análise de informações. Estamos na era do "Big Data" e da "Internet das Coisas", o que nos deixa vulneráveis à ingerência de diversas empresas.

O direito à liberdade envolve diferentes manifestações, em função das atividades desenvolvidas pelo homem, nos níveis pessoais, negociais e espirituais. O bem jurídico protegido é a liberdade, que se pode definir como a faculdade de

fazer, ou deixar de fazer, aquilo que a ordem jurídica permita. É a prerrogativa que a pessoa tem para desenvolver, sem obstáculos, suas atividades no mundo das relações. O ordenamento jurídico confere-lhe, para tanto, a necessária proteção nos pontos considerados essenciais à personalidade humana, como a locomoção, o pensamento e sua expressão, o culto, a comunicação em geral, entre outros. Ora, em uma Sociedade da Informação, como a que atualmente vivemos, a internet é instrumento fundamental para exercício da liberdade de expressão. As redes sociais tornaram-se ferramenta hábil em dar voz e publicidade para diversas parcelas da população, tornando efetivo o exercício da democracia.

Todos os direitos citados acima possuem previsão expressa na Constituição Federal de 1988, no Código Civil Brasileiro, além do próprio Marco Civil da Internet (Lei nº 12.965/2014), que servem como meios de proteção, garantia e resguardo desses e de outros direitos fundamentais. A título de exemplo, citamos aqui o artigo 3º da referida lei, que expressamente adota como princípios para disciplina do uso da internet a garantia da liberdade de expressão e a proteção da privacidade dos dados pessoais.

Pesquise mais

Sobre os direitos fundamentais do usuário na internet, consolidados pelo Marco Civil da Internet, recomendamos a leitura do seguinte artigo: MOLON, Alessandro. **Marco Civil da Internet**: a garantia de direitos fundamentais do usuário. Disponível em: <http://www.oabrj.org.br/materia-tribuna-do-advogado/18113-marco-civil-da-internet-a-garantiade-direitos-fundamentais-do-usuario>. Acesso em 30 abr. 2016.

Sem medo de errar

Vamos retomar nossa situação-problema? Ao desenvolver a rede social, o dono da empresa pediu que você pontuasse e analisasse os principais direitos fundamentais dos usuários com os quais a empresa deve se preocupar ou dar mais atenção. Dentre os vários direitos fundamentais, quais são aqueles que, na prática, apresentam maior vulnerabilidade na internet?

Atenção

Para resolvermos a situação-problema proposta, devemos resgatar o conceito e delimitação de direitos fundamentais, e quais os principais diplomas legais que protegem tais direitos.

Os direitos fundamentais que apresentam maior vulnerabilidade na internet são a honra, a privacidade e a liberdade, previstos no artigo 5º da Constituição Federal de 1988, e que são também direitos da personalidade, previstos no Código Civil Brasileiro, e que ainda estão consolidados na Lei nº 12.965/2014, do Marco Civil da internet.

O direito à honra refere-se à necessidade de defesa da reputação da pessoa (física ou jurídica), compreendendo o bom nome e a fama de que desfruta perante a coletividade, enfim, a estima que a cerca nos seus ambientes, familiar, profissional, comercial ou outro. Alcança também o sentimento pessoal de estima, ou a consciência da própria dignidade. O direito à privacidade, ou intimidade, refere-se ao direito que a pessoa tem de se resguardar contra injunções, indiscrições ou intromissões alheias. O direito à liberdade envolve diferentes manifestações, em função das atividades desenvolvidas pelo homem, nos níveis pessoais, negociais e espirituais. O bem jurídico protegido é a liberdade, que se pode definir como a faculdade de fazer, ou deixar de fazer, aquilo que a ordem jurídica permita.

Essa vulnerabilidade se justifica em razão do papel catalisador que o meio eletrônico exerce. A publicação de um conteúdo ofensivo é visualizada por milhares de pessoas em diferentes lugares; uma empresa, como Facebook ou Google, possui um "mar" de dados pessoais de usuários, os quais ficam expostos às ingerências por parte desses e de outros provedores. Preceitos como "honra", "privacidade" e "liberdade de expressão" nunca foram tão relevantes e ao mesmo tempo vulneráveis.

Avançando na prática

Delimitando Direitos Fundamentais

Descrição da situação-problema

Você, renomado consultor de TI, foi contratado por uma empresa de telefonia para emitir um parecer fundamentado, de modo a dizer se o direito do usuário de não ter suspenso sua conexão à internet, em caso de esgotamento de sua franquia de dados de celular, caracteriza-se como um direito fundamental.

Lembre-se

Ao delimitarmos e, consequentemente, conceituarmos um direito fundamental, devemos analisar tanto seu aspecto formal (onde está previsto?) quanto seu aspecto material (o que está previsto?). Lembrando ainda que direitos fundamentais são aqueles que têm como principal finalidade proteger a dignidade humana em todas as dimensões.

Resolução da situação-problema

Como vimos, pelo critério formal de identificação, os direitos fundamentais seriam aqueles inseridos em instrumentos internacionais, tais como convênios, protocolos, constituições, tratados etc.

Esse critério, contudo, não é suficiente para delimitarmos um direito fundamental, pois tal sistematização pode suscitar dúvidas, por exemplo, sobre se todos os direitos consagrados nas constituições no título próprio são fundamentais ou não.

Doutro lado, se considerarmos a existência de um critério objetivo do ponto de vista material, os direitos fundamentais são, em geral, aquelas prerrogativas das pessoas, que se consideram de maior importância no ordenamento jurídico. Em outras palavras, é um direito fundamental do ponto de vista material, se sua existência tem um grau de necessidade que, sem ele, não se poderia desenvolver determinada concepção do Estado e da sociedade.

Assim, importaria averiguar quais seriam os direitos que podem ser tidos como absolutamente necessários, conferindo a eles, assim, um caráter "fundamental". O Brasil adota uma espécie de teoria "mista". Nesse sentido, o simples fato do direito a "não suspensão da conexão" não estar previsto na Constituição, não significa que ele não seja um direito fundamental. Devemos analisar o teor da norma, ou seja, se é um direito indispensável ao exercício da democracia. Ora, em que pese ser uma garantia do usuário de internet, não podemos afirmar ser este um direito fundamental, pois, não expressa uma norma indispensável ao cidadão, do ponto de vista objetivo. Além disso, tal direito não se encontra consagrado na Constituição nem em outros diplomas internacionais que contemplam outros direitos fundamentais, como a Declaração Universal dos Direitos Humanos.

Faça você mesmo

Para aprofundar seus conhecimentos, sugerimos que você leia o artigo 5º da Constituição Federal Brasileira em sua integralidade, conhecendo outros direitos fundamentais que não só aqueles trabalhados nesta seção. Além de aumentar seus conhecimentos, você se tornará um cidadão mais completo, consciente dos limites de atuação do Estado dentro de um regime democrático.

Faça valer a pena

1. Considere as seguintes afirmativas:

I – Os direitos fundamentais reconhecidos por um Estado são a melhor

via para constatar seu caráter democrático ou não, liberal ou social.

II – Após a popularização da internet e o advento das redes sociais e do comércio eletrônico, a necessidade de proteger os direitos fundamentais aumentou consideravelmente, tendo em vista o papel catalisador que o meio eletrônico exerce.

III – O alcance e grau de exigibilidade dos direitos fundamentais, assim como as transformações que ocorrem no sistema jurídico em consequência de sua positivação constitucional, são tratados como consenso pela doutrina.

Estão corretas as afirmativas:

a) I, apenas.

b) I e II.

c) I e III.

d) II e III.

e) I, II e III.

2. Sobre a delimitação dos direitos fundamentais, considere as seguintes afirmativas:

I – Um direito fundamental é, do ponto de vista do critério material, aquele cuja existência tem um grau de necessidade que, sem ele, não se poderia desenvolver determinada concepção do Estado e da sociedade.

II – O critério formal é suficiente para delimitarmos um direito fundamental, pois todos os direitos consagrados nas constituições possuem caráter fundamental.

III – Pelo critério formal de identificação, os direitos fundamentais seriam aqueles inseridos em instrumentos internacionais, tais como convênios, protocolos, constituições, tratados etc. (Exemplificando: A Declaração Universal dos Direitos Humanos é um documento internacional, ratificado por vários países e que define e protege diversos direitos fundamentais).

Estão corretas as afirmativas:

a) I, apenas.

b) I e II.

c) I e III.

d) II e III.

e) I, II e III.

3. Sobre a proteção dos direitos fundamentais, considere as seguintes afirmativas:

I – Os direitos fundamentais são protegidos tanto por normas constitucionais quanto infraconstitucionais (ex.: Marco Civil da Internet).

II – A Constituição Federal serve como bússola para delimitarmos o caráter "fundamental" de um direito, sobretudo, em razão do fenômeno da "constitucionalização" dos direitos fundamentais.

III – A Constituição Federal de 1988 é o único diploma legal responsável por proteger os direitos fundamentais de eventuais abusos e violações.

Estão corretas as afirmativas:

a) I, apenas.

b) I e II.

c) I e III.

d) II e III.

e) I, II e III.

Seção 2.2

Resolução de conflitos entre direitos fundamentais

Diálogo aberto

Na última seção estudada, vimos o importante papel que os direitos fundamentais exercem na formação de uma internet mais democrática. Igualmente, destacamos três direitos fundamentais que, constantemente, entram em rota de colisão no ambiente on-line, quais sejam, honra, privacidade e liberdade de expressão. Nesse contexto, é muito comum que de um lado fique a liberdade de expressão e, do outro, a honra ou a privacidade. Assim, é possível afirmarmos que a liberdade de expressão está sempre em destaque, sendo alvo de usual limitação por parte das autoridades públicas. Trata-se de uma batalha interminável. Tal disputa ganhou corpo principalmente após o advento da web 2.0, caracterizada pela difusão de tecnologias, como as redes sociais e os blogs. Porém, como balancear os interesses envolvidos? Qual o limite da proteção da liberdade de expressão, da honra e da privacidade?

Antes de nos aprofundarmos nesta e em outras questões, vamos retomar nossa situação geradora de aprendizagem (SGA)? Suponhamos que você foi contratado por uma empresa que possui um website, onde diariamente publica conteúdos relacionados à cultura pop. A empresa deseja desenvolver uma plataforma de rede social para que seus usuários interajam entre si e compartilhem conteúdos diversos. Seu trabalho consiste também em realizar a blindagem jurídica desta nova aplicação, conforme explicado anteriormente.

Para esta seção, iremos considerar a seguinte situação-problema: Ao desenvolver a rede social, o dono da empresa, ciente dos principais direitos fundamentais aos quais a empresa deve se atentar, pediu que, em uma reunião com possíveis investidores, você explicasse como funciona a resolução de conflitos entre direitos fundamentais, de modo a diminuir a preocupação dos investidores com eventuais abusos de usuários ou autoridades governamentais. Para resolver a situação, iremos estudar os critérios de resolução de conflitos entre direitos fundamentais, com especial destaque para o princípio da proporcionalidade, analisando ainda situações concretas, como a interceptação de mensagens eletrônicas, e como deve o Judiciário agir de modo a minimizar os danos para os usuários.

Não pode faltar

Conforme vimos na Seção 2.1, os direitos fundamentais, apesar de serem importantíssimos na formação de um Estado Democrático de Direito, não são absolutos. Esses preceitos possuem caráter relativo, ou seja, sujeitam-se às restrições impostas pelo próprio legislador ou pelo julgador ao serem invocados em ação judicial.

Norberto Bobbio (1992, p. 40) observa que, entre os direitos fundamentais, raros são aqueles que não entram em concorrência com outros direitos fundamentais, que não são suspensos em determinadas circunstâncias ou que não são negados a determinadas categorias de pessoas, por isso se diz que não possuem caráter absoluto.

Em análise à Constituição Federal de 1988, identificam-se possíveis colisões entre direitos fundamentais, o que demonstra a necessidade de se admitir seu caráter relativo como única forma de resolução dos conflitos nos casos concretos. O professor Edilson Farias (2000, p. 116) nos ensina que, em se tratando de colisões entre direitos fundamentais e de direitos fundamentais com a necessidade de preservação de um bem coletivo ou do Estado, tal colisão pode se dar de duas maneiras distintas:

(1) o exercício de um direito fundamental colidindo com o exercício de outro direito fundamental (colisão entre os próprios direitos fundamentais);

(2) o exercício de um direito fundamental colidindo com a necessidade de preservação de um bem coletivo ou do Estado, protegido constitucionalmente (colisão entre direitos fundamentais e outros valores constitucionais).

O professor Norberto Bobbio ainda complementa sua ideia de "ilusionismo" quanto ao caráter absoluto dos direitos fundamentais, no sentido de que não poderiam ser relativizados ou mitigados em hipótese nenhuma, com o argumento de que a história demonstra que os direitos fundamentais formam uma classe variável no tempo e no espaço. Nesse sentido, direitos que foram declarados absolutos e invioláveis no final do século XVIII, como à propriedade, foram submetidos a radicais limitações nas declarações contemporâneas, e 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 em outras culturas.

O argumento de Bobbio é perfeitamente aplicável nos dias de hoje, eis que

o desenvolvimento de novas tecnologias, principalmente no ramo informacional, fomenta a violação de determinados direitos fundamentais, tendo como justificativa o próprio exercício de outros direitos fundamentais.

Exemplificando

As novas situações jurídicas no ambiente virtual são provas incontestáveis dessa tendência de fomento da violação de direitos fundamentais sob o argumento de exercício de outro direito fundamental. Toma-se, a título de exemplo, o envio indiscriminado de e-mails (spam) por meio da internet em face da privacidade do usuário (privacidade X liberdade de expressão).

Em suma, apesar da essencialidade e da "fundamentalidade" nos ordenamentos jurídicos, podemos concluir que os direitos fundamentais têm, intrinsecamente, caráter relativo, submetendo-se às restrições impostas pelo legislativo – no momento da conformação legislativa – e pelo judiciário – no momento da resolução dos casos concretos.

Tal situação, como não poderia deixar de ser, estende-se também aos direitos de privacidade, honra e liberdade de expressão. Embora o texto constitucional brasileiro resguarde tais direitos, observa-se na jurisprudência a frequente mitigação desses preceitos fundamentais diante da necessidade de preservação de um ou outro interesse que logra preponderar, o que demonstra o caráter relativo dos referidos direitos. E como resolver eventuais conflitos entre os direitos acima citados, direitos que possuem o mesmo "nível hierárquico", ou seja, previstos na Constituição? Lembre-se que, em seções anteriores, vimos conteúdos que se relacionam aqui. Este é o momento de você relembrá-los.

A respeito da colisão de princípios, nos ensina o jurista e filósofo Alexy (2002, p. 89) que quando dois princípios entram em colisão, um dos dois princípios tem que ceder ante o outro. Isto 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. Isto é, em determinadas situações, a privacidade se sobreporá 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.

Assimile

Havendo colisão entre direitos fundamentais, 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 do usuário. 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 da polícia, chegando 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.

Podemos dizer que o princípio da proporcionalidade consiste na verificação pelo juiz, quando diante de dois interesses, se estes 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 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 é justamente salvaguardar o núcleo essencial dos direitos e garantias previstos em Constituição.

Reflita

Qual a importância do princípio da proporcionalidade na hipótese de conflitos entre princípios constitucionais? Pode-se dizer, seguramente, que é buscar o ponto de equilíbrio entre os interesses em jogo e que, aparentemente, se encontram em situação de conflito. Para o tema em análise, é ainda verificar se as medidas para a solução do problema apresentam-se necessárias, razoáveis e sem excessos, de modo que não existam outros meios, menos invasivos, capazes de solucionar os problemas advindos daquele conflito.

A questão da análise de excessos torna-se particularmente importante quando tratamos da liberdade de expressão no ambiente on-line. Como sabemos, esse é um direito previsto em nossa Constituição, especificamente no artigo 5º, inciso IV. Entretanto, tal direito, como vimos, não pode ser considerado absoluto, sofrendo restrições tanto sob a ótica do princípio da proporcionalidade, em caso de conflito com outros direitos igualmente previstos na Constituição (ex.: honra e privacidade), quanto do próprio texto legal. Nesse sentido, o próprio inciso IV impõe uma condição ao exercício da liberdade de expressão, que é a vedação ao anonimato. Assim, podemos exercer tal direito dentro de certos limites, sendo necessário, ainda, nos identificarmos. Neste estágio é importante diferenciarmos "anonimato" de privacidade. Anonimato é a falta de possibilidade de identificação, já a privacidade é o direito ao resguardo de certas informações contra revelação não autorizada.

A fim de contextualizarmos o tópico tratado ao longo desta seção, cumpre relembrarmos alguns episódios recentes ocorridos no Brasil. Por duas vezes, o aplicativo WhatsApp foi bloqueado por dois magistrados diferentes sob o argumento de que a empresa Facebook, como legítima titular da aplicação no território brasileiro, recusou-se a fornecer determinados dados, considerados sigilosos, acerca de seus usuários. Dados estes requisitados pelas autoridades no contexto de uma investigação criminal.

Analisando referida situação concreta, temos, de um lado, a privacidade dos usuários da aplicação, que, conforme a Constituição e o Marco Civil da Internet, têm o direito de resguardar a privacidade de seus dados, notadamente o conteúdo das mensagens trocadas entre si, das ingerências do Estado. Por outro lado, temos o direito legítimo do Estado e, consequentemente, de seus representados (cidadãos) de ver protegida a "segurança nacional", ou seja, de serem investigados e punidos aqueles que contrariam a ordem nacional. Lembrando que a aplicação foi utilizada pelos criminosos para efetuar negociações envolvendo tráfego de entorpecentes ilícitos.

Ao decidir, ambos os magistrados entenderam por bem aplicar a sanção prevista no artigo 12 do Marco Civil da Internet, que prevê a possibilidade de bloqueio temporário da aplicação. Apesar de, aparentemente, legítima, a decisão foi duramente criticada, ao passo que privou o acesso de 100 milhões de usuários ao aplicativo. Ora, entendemos que, ao decidir, os magistrados não observaram com o devido cuidado o critério de proporcionalidade para resolução de tal conflito entre valores fundamentais (privacidade X segurança nacional).

Para verificar a proporcionalidade do bloqueio adotado, devemos analisar se a medida para solução do problema foi necessária, razoável e sem excesso, e ainda, se não existiam outros meios, menos invasivos, capazes de solucionar os problemas advindos do conflito. Em primeira análise, podemos concluir que a

medida foi excessiva, ao passo que privou do acesso ao aplicativo milhões de usuários, prejudicando suas rotinas. Foi o bloqueio necessário? Ao nosso ver, não, pois existem outros remédios jurídicos, inclusive previstos no próprio Marco Civil da Internet, menos danosos à sociedade e ao mercado, como a aplicação de multa sobre o faturamento líquido da empresa. Por fim, existem outras medidas menos danosas para a solução do problema, como a requisição dos dados via acordo de cooperação bilateral, em que a autoridade brasileira roga à autoridade estrangeira o envio dos dados necessários.

Pesquise mais

Para saber mais sobre a "proporcionalidade" (ou não) das decisões relativas ao bloqueio de aplicações, recomendamos a leitura do artigo "Bloqueio do WhatsApp revela desapreço pela liberdade de Comunicação". Disponível em: <http://www.estadao.com.br/noticias/geral,analise---bloqueio-de-whatsapp-revela-desapreco-pela-liberdade-de-comunicacao,10000048895>. Acesso em: 11 jul. 2016.

Sem medo de errar

Apresentados os fundamentos da seção, vamos resolver nossa situação-problema? Ao desenvolver a rede social, o dono da empresa, ciente dos principais direitos fundamentais aos quais a empresa deve se atentar, pediu que, em uma reunião com possíveis investidores, você explicasse como funciona a resolução de conflitos entre direitos fundamentais, de modo a diminuir a preocupação dos investidores com relação a eventuais abusos de usuários ou autoridades governamentais.

Atenção

Não existem direitos fundamentais absolutos. Estes possuem caráter relativo e, no caso concreto, deve o julgador atentar-se para o caso concreto, norteando-se pelo princípio da proporcionalidade.

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. 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. Isto é, em determinadas situações a privacidade se sobreporá 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.

Tal avaliação deve se basear em um critério de proporcionalidade. Podemos dizer que o princípio da proporcionalidade consiste na verificação pelo juiz, diante de dois interesses legitimamente tuteláveis e em conflito, se estes são, com efeito, juridicamente protegidos. Em caso afirmativo, deverão os 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, não devendo sempre prevalecer a predominância da busca da verdade no processo, sobre o direito ao resguardo e vice-versa. Cabe ao julgador, através da análise minuciosa dos interesses, decidir em que medida deve-se fazer prevalecer, a despeito de eventuais inconvenientes, um ou outro interesse legitimamente tutelável pelo Direito, impondo restrições necessárias ao resguardo de outros bens jurídicos.

Avançando na prática

O problema do bloqueio de aplicações na internet

Descrição da situação-problema

Você, empreendedor da área de tecnologia, juntamente com uma equipe qualificada, criou um aplicativo de troca de mensagens instantânea entre usuários. Logo, tal aplicação ganhou nome no mercado, alcançando o patamar de um milhão de usuários. Certo dia, você foi surpreendido com uma intimação judicial, determinando que fornecesse dados referentes às mensagens privadas de certos usuários, que estavam sendo investigados criminalmente, sob pena de bloqueio do aplicativo. Caso você e sua empresa se recusasse a fornecer tais dados, em respeito à privacidade de seus usuários, eventual bloqueio da aplicação poderia ser considerado legítimo? Seria a decisão proporcional?

Lembre-se

O Marco Civil da Internet prevê, em seu artigo 12, uma série de sanções em caso de descumprimento de ordem judicial. Igualmente, em seu artigo 15, temos que o provedor de aplicação deve armazenar os registros de acesso à aplicação, como números de IP, nome de usuário, horas de login e logout.

Resolução da situação-problema

O artigo 12 do Marco Civil da Internet (Lei nº 12.965/2014) prevê a possibilidade de bloqueio temporário da aplicação, assim, eventual decisão, bloqueando o aplicativo é, a princípio, legítima. Para verificar a proporcionalidade de eventual bloqueio, devemos analisar se a medida para solução do problema é necessária, razoável e sem excesso, e ainda se não existem outros meios, menos invasivos,

capazes de solucionar o problema. Em primeira análise, podemos concluir que a medida é excessiva, ao passo que priva do acesso ao aplicativo outros usuários, prejudicando suas rotinas. Se não bastasse, existem outros remédios jurídicos, inclusive previstos no próprio Marco Civil da Internet, menos danosos à sociedade e ao mercado, como a aplicação de multa sobre o faturamento líquido da empresa. Portanto, uma decisão desse tipo pode ser considerada desproporcional, apesar de legítima.

Faça você mesmo

Se você entende que decisões como o bloqueio do aplicativo WhatsApp são desproporcionais, você pode fazer abaixo-assinados para tentar barrar tal prática, ou mesmo, assinar um e deixar seu comentário no endereço a seguir. Disponível em: <https://www.change.org/p/bloqueio-n%C3%A3o-a-internet-no-brasil-deve-ser-livre>. Acesso em: 11 jul. 2016.

Faça valer a pena

1. Sobre os direitos fundamentais e seu caráter relativo, assinale a alternativa incorreta:

a) Por serem importantes na formação de um Estado Democrático de Direito, os direitos fundamentais são absolutos.

b) Os direitos fundamentais sujeitam-se às restrições impostas pelo próprio legislador ou pelo julgador ao serem invocados em ação judicial.

c) Em análise à Constituição Federal de 1988, identificam-se possíveis colisões entre direitos fundamentais, o que demonstra a necessidade de admitir seu caráter relativo como única forma de resolução dos conflitos nos casos concretos.

d) Para Norberto Bobbio, entre os direitos fundamentais, raros são aqueles que não entram em concorrência com outros direitos fundamentais, por isso se diz que não possuem caráter absoluto.

e) Os direitos fundamentais podem sofrer restrições, devendo o julgador ater-se à análise do caso concreto.

2. Acerca dos ensinamentos do professor Norberto Bobbio, considere as seguintes afirmativas:

I – A ideia de "ilusionismo" do caráter absoluto dos direitos fundamentais

é comprovada pela própria história, que demonstra que os direitos fundamentais formam uma classe variável no tempo e no espaço.

II – 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.

III – Os direitos fundamentais não entram em concorrência com outros direitos fundamentais, não são suspensos em determinadas circunstâncias e não são negados a determinadas categorias de pessoas, por isso, são considerados absolutos.

É correto aquilo que se afirma em:

a) I, apenas.

b) I e II.

c) I e III.

d) II e III.

e) I, II e III.

3. Sobre a colisão entre direitos fundamentais, considere as seguintes afirmativas:

I – Conforme o jurista e filósofo Alexy, quando dois princípios entram em colisão, um deles tem que ceder ante o outro. Mas isto não significa declarar inválido o princípio "desprezado".

II – Por estarem previstos no texto constitucional brasileiro, a jurisprudência nega a mitigação dos direitos fundamentais, mesmo diante da necessidade de preservação de um ou outro interesse, vez que tais direitos, em hipótese nenhuma, entram em conflito.

III – Havendo colisão entre direitos fundamentais, 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, considerando o caso concreto.

É correto aquilo que se afirma em:

a) I, apenas.

b) I e II.

c) I e III.

d) II e III.

e) I, II e III.

Seção 2.3

Responsabilidade civil na internet

Diálogo aberto

Na primeira metade desta Unidade de estudo, vimos questões relacionadas aos Direitos Fundamentais, seu conceito, natureza, bem como os critérios de resolução de conflitos envolvendo esses direitos que, de maneira recorrente, colidem entre si no ambiente on-line. Para o estudo da presente seção, é importante notarmos que sempre que os direitos fundamentais colidem entre si, uma das partes, na grande maioria das vezes, é prejudicada, o que resulta em um dano à pessoa, podendo tal dano ser de ordem moral ou material. Ocorrendo um dano, como se dá a responsabilização da parte ofensora, ou ainda, da parte que colaborou para aquele dano? Estes questionamentos são pertinentes nos dias de hoje, tendo em vista que constantemente somos expostos a abusos na internet, seja por partes de pessoas mal-intencionadas ou por empresas que não se preocupam com o bem-estar e segurança de seus clientes e consumidores.

Retomemos nossa situação-geradora de aprendizagem (SGA): Suponhamos que você foi contratado por uma empresa que possui um website, no qual diariamente são publicados conteúdos relacionados à cultura pop. A empresa deseja desenvolver uma plataforma de rede social para que seus usuários interajam entre si e compartilhem conteúdos diversos. Seu trabalho consiste também em realizar a blindagem jurídica desta nova aplicação, conforme explicado.

Para esta seção, consideremos a seguinte situação-problema: No desenvolvimento da plataforma de rede social, ficou decidido que serão armazenados, por um período determinado, diversos dados pessoais dos usuários da aplicação, como nome, endereço, telefone e e-mail. Porém, a fim de tomar medidas de segurança e proteção dos referidos dados, o diretor de TI pediu que você analisasse a questão da responsabilidade da empresa por eventuais incidentes envolvendo o vazamento desses dados e, ainda, se existem medidas capazes de atenuar eventual responsabilidade.

Para resolver a situação-problema proposta, iremos estudar a questão da responsabilidade civil em nosso ordenamento jurídico, os pressupostos da responsabilidade civil, suas espécies e hipóteses excludentes. A partir daí, estaremos

habilitados para responder os questionamentos propostos, sobretudo qual a responsabilidade da empresa nesse caso e quais as medidas para mitigação de riscos.

Não pode faltar

O instituto da responsabilidade civil integra o chamado "direito das obrigações", que resulta na obrigação de reparar eventual dano ocasionado. Essa obrigação é de natureza pessoal e resolve-se em perdas e danos conforme dispõe o atual Código Civil em seu artigo 389. Quem pratica um ato, ou incorre numa omissão da qual resulte dano, deve suportar as consequências do seu procedimento.

Assimile

A responsabilidade civil pode ser entendida como verdadeira ferramenta para o restabelecimento de um equilíbrio social. Nesse sentido, aquele que causa um dano tem o dever legal de repará-lo.

Os elementos ou pressupostos gerais da responsabilidade civil são os seguintes: ato ou conduta; dano ou prejuízo; e o nexo de causalidade entre o ato e o dano. O primeiro elemento (ato) refere-se justamente a uma ação ou omissão da própria pessoa, por ato de terceiro (ex.: pais respondendo pelos atos dos filhos), ou por fato de coisa ou animal (ex.: o dono de um animal responde pelos danos causados por este a um terceiro).

Exemplificando

Um exemplo de responsabilidade pelo fato de coisa é, justamente, quando adquirimos um produto que apresenta algum vício ou defeito. Nestes casos, podemos acionar judicialmente o vendedor ou fabricante daquele produto requerendo sua substituição ou indenização em valor equivalente.

O segundo elemento em estudo (dano) refere-se à lesão a um interesse juridicamente protegido, podendo ser de ordem moral ou material. O dano, mesmo que moral, deve ser certo, ou seja, deve necessariamente ter que existir. Já o terceiro elemento (nexo causal) é um vínculo que liga a conduta ou ato ao resultado danoso. Sem essa relação de causalidade, não se pode admitir a existência de uma obrigação de indenizar.

Historicamente, o Código Civil de 1916, no artigo 159, consagrou a regra geral da responsabilidade subjetiva, também chamada no mundo jurídico de

responsabilidade aquiliana, prescrevendo que aquele que por ação ou omissão voluntária, negligência ou imprudência violar um direito ou causar prejuízo a outrem, fica obrigado a reparar o dano. Hoje em dia, o Código Civil de 2002 prevê tal obrigação em seu artigo 927. Ou seja, havendo culpa, mesmo que levíssima, há obrigação de indenizar.

Por sua vez, a industrialização e o surgimento de novas tecnologias intensificaram o aumento de acidentes ou eventos danosos, o que motivou uma nova análise da responsabilidade civil, que passou a ser vista sob o prisma da "teoria do risco". Falamos hoje em responsabilidade objetiva, no sentido de que não se exige o elemento culpa para que se configure a obrigação de indenizar. Entretanto, trata-se de verdadeira exceção à regra, contida no citado artigo 927, que decorre de certas relações especiais, em que há uma espécie de desequilíbrio entre as partes (ex.: relação entre empresas e consumidores).

Com a popularização da internet, grande parte das atividades sociais contemporâneas foram transportadas para o meio eletrônico. Hoje em dia, pagamos contas pela internet, compramos produtos e, inclusive, nos relacionamos com terceiros também neste meio. Assim, foram criados novos desafios jurídicos, ligados justamente à responsabilidade pelos danos causados neste ambiente.

A questão principal quando o assunto é internet diz respeito a quem atribuir a culpa e eventual responsabilidade pelo dano. Por muito tempo se discutiu o papel dos fornecedores de serviços na internet, especificamente a questão da responsabilidade destes pelos atos cometidos por seus usuários. Entretanto, este assunto será analisado com maiores detalhes na próxima sessão.

Nesta sessão, iremos focar principalmente nas duas categorias de responsabilidade civil acima expostas, quais sejam, a responsabilidade subjetiva e a responsabilidade objetiva, aplicadas a um contexto de internet.

Como dissemos anteriormente, a regra da responsabilidade civil subjetiva, ou aquiliana, imposta pelo artigo 159 do Código Civil de 1916 e reproduzida pelo artigo 186 e 927 do atual Código de 2002, prevalece como princípio geral. Entretanto, a lei introduziu o instituto da responsabilidade objetiva, ampliando o conceito de culpa. Portanto, existindo dano, socialmente relevante, e não sendo possível provar a culpa, a lei, em algumas circunstâncias, dispensa esta prova, desde que presente o nexo de causalidade.

Primeiramente, iremos analisar as várias modalidades de culpa dentro de um contexto de internet e ambiente eletrônico, lembrando que a culpa se refere justamente à caracterização da responsabilidade subjetiva. Iremos estudar cinco diferentes modalidades de culpa, contextualizando-as. Para tanto, iremos utilizar uma situação muito comum em nosso cotidiano, as fraudes bancárias.

A primeira refere-se à *culpa in eligendo*, ou a culpa decorrente da escolha ou opção pelos serviços. Em nosso contexto de fraude bancária, podemos dizer que o banco prestador de serviços em ambiente eletrônico (ex.: *Internet Banking*) terá culpa se houver adquirido recursos informáticos inadequados, ou seja, caso não tenha adotado cuidados razoáveis na escolha de tais recursos, como consultorias especializadas e tecnologias adequadas para proteger seus clientes.

A segunda relaciona-se à *culpa in vigilando*, que é a culpa em razão da violação de um dever de vigilância. Em nosso exemplo, trata-se do dever do banco de realizar uma vigilância mínima sobre as transações efetuadas por seus clientes. Não se trata de uma vigilância sobre todas as operações, o que poderia resultar também em violação à privacidade de seus clientes, trata-se da vigilância, por exemplo, de transações estranhas e incomuns. Algumas instituições fazem isso, entrando em contato com seus clientes em caso de compras suspeitas realizadas com cartão de crédito pela internet.

A terceira refere-se à *culpa in omittendo*, ou culpa decorrente da omissão de informações relevantes. Este é um tópico polêmico, tendo em vista uma variação muito grande entre o nível de informação dos próprios usuários. Assim, a omissão deve ser analisada com cautela, limitando-se essencialmente a questões de segurança.

A quarta relaciona-se à *culpa in custodiendo*, que trata da culpa pela violação do dever de guarda ou custódia. Trata-se, por exemplo, da responsabilidade do banco em relação à guarda de dados de seus usuários. Deve a instituição garantir a integridade de tais dados adotando medidas proativas, como criptografia, firewalls etc.

Por último, temos a quinta modalidade que é a *culpa in contraendo*. Trata-se de modalidade semelhante à *culpa in eligendo*, mas diz respeito à responsabilidade por cumprir com aquilo que foi prometido. Para nosso exemplo, trata-se do dever do banco de ofertar serviços com segurança mínima razoável. Caso não estejam presentes tais requisitos, não deve a instituição contratar com possíveis interessados.

Quanto à aplicação da "teoria do risco" aos eventos danosos ocorridos no meio eletrônico, por muito tempo discutiram-se os riscos atribuíveis à responsabilidade de cada parte. O conceito de risco liga-se ao dano, não de qualquer dano, mas de dano certo e atual. Mas tal caracterização nem sempre é fácil. Como medir tais riscos, de modo a dizer se estes são ou não aceitáveis e em que medida?

Reflita

Como enquadrar os danos certos e atuais de uma rede eletrônica pelo simples fato de saber que ela pode ser alvo de ataques de vírus que,

> uma vez realizados, são programados para produzir resultados em data futura? Seriam estes danos certos e atuais? Para respondermos tal questionamento, devemos analisar o estágio tecnológico do mercado em determinado momento.

Para tanto, devemos recorrer novamente à proporcionalidade ou razoabilidade. Ou seja, considerando o estado da técnica da maioria das empresas em um determinado momento, é razoável admitir que determinado risco era previsível? Em caso positivo, é possível cogitarmos a responsabilização objetiva do agente causador do dano.

Como dissemos, o Código Civil não tratou especificamente da responsabilidade civil na internet ou no meio eletrônico, mas algumas disposições adaptam-se perfeitamente ao caso. Nessa esteira, o Código de Defesa do Consumidor tem tido fundamental importância no tocante à aplicação da responsabilidade objetiva no campo da informática.

Por fim, existem situações especiais nas quais os agentes causadores do dano não possuem responsabilidade de indenizar referido dano. Tratam-se das chamadas causas excludentes de responsabilidade civil. A lei prevê causas que afastam a responsabilidade do agente por diferentes razões, como: o estado de necessidade, a legítima defesa, o exercício regular do direito, o estrito cumprimento do dever legal; o caso fortuito ou força maior, a culpa exclusiva da vítima ou o fato de terceiro (GAGLIANO; PAMPLONA FILHO, 2011, p. 143).

As causas excludentes de responsabilidade civil são situações que, ao ocorrer, tendo como resultado um dano, não geram, contra o agente, pretensões indenizatórias, atacando diretamente os elementos da responsabilidade civil, fazendo-a inexistir. Acontece sempre que há um fato externo que leva a ocorrer algo que, mesmo diante de ação ou omissão do agente, não se originou de sua própria vontade, ou seja, não foi espontânea, não nasceu de sua autodeterminação (GAGLIANO; PAMPLONA FILHO, 2011, p. 143).

A fim de compreendermos um pouco mais as causas excludentes da responsabilidade civil, cumpre tecermos algumas considerações sobre cada uma das causas anteriormente citadas.

- Estado de necessidade: neste caso, o agente é obrigado, em razão de determinadas circunstâncias que o cercam, a "sacrificar" um bem jurídico;
- Legítima defesa: aqui, o sujeito repele uma agressão injusta praticada contra um bem jurídico próprio ou de terceiro;
- Exercício regular do direito: nesta hipótese, o sujeito atua amparado por um direito legítimo e reconhecido, e que em razão deste direito, não poderá ser atacado ou repreendido;

- Estrito cumprimento do dever legal: muito semelhante ao exercício regular do direito, esta hipótese refere-se ao exercício de um dever legalmente previsto. Aplica-se principalmente para o caso de agentes públicos;
- Caso fortuito ou força maior: o caso fortuito decorre de forças da natureza, tais como terremoto, inundação e incêndio não provocado, enquanto a força maior decorreria de atos humanos inelutáveis, tais como guerras, revoluções, greves e determinação de autoridades;
- Culpa exclusiva da vítima: é a culpa ou fato exclusivo da vítima, circunstância que exime completamente a responsabilidade do agente;
- Fato de terceiro: é o instituto excludente de nexo causal que se constitui quando o dano se dá por ato de terceiro, sendo o suposto agente um mero instrumento para a causalidade.

Pesquise mais

Caso queira se aprofundar nas questões relativas às causas excludentes de responsabilidade civil, sugerimos a leitura do artigo. Disponível em: <http://apenassobredireito.blogspot.com.br/2013/10/causas-excludentes-de-responsabilidade.html>. Acesso em: 11 jul. 2016.

Sem medo de errar

Apresentados os principais conceitos sobre responsabilidade civil, vamos resolver nossa situação-problema? No desenvolvimento da plataforma de rede social, ficou decidido que serão armazenados, por um período determinado, diversos dados pessoais dos usuários da aplicação, como nome, endereço, telefone e e-mail. Porém, a fim de tomar medidas de segurança e proteção dos referidos dados, o diretor de TI pediu que você analisasse a questão da responsabilidade da empresa por eventuais incidentes envolvendo o vazamento desses dados e, ainda, se existem medidas capazes de atenuar eventual responsabilidade.

Atenção

Neste caso, entre a empresa que disponibiliza seus serviços na internet e seus usuários existe verdadeira relação de consumo, inclusive se os serviços oferecidos forem gratuitos. Isto porque, de acordo com a jurisprudência de nossos Tribunais Superiores, existe uma relação

de ganho indireto, ou cross marketing, quando o ganho não advém do pagamento pelos consumidores, mas em razão de anúncios e patrocínios de terceiros. Dessa maneira, a empresa responderá objetivamente por eventuais defeitos em seus serviços.

A princípio, podemos afirmar que a responsabilidade da empresa por eventuais incidentes envolvendo o vazamento de dados pessoais de seus usuários possui o caráter objetivo. Isto porque entre a empresa e seus usuários existe verdadeira relação de consumo, atraindo, assim, as normas do Código de Defesa do Consumidor e, por consequência, a responsabilização objetiva pelos defeitos nos produtos. Todavia, a fim de afastar tal responsabilização objetiva e subsidiar uma tese de responsabilidade subjetiva, ou mesmo uma defesa que sustente uma exclusão de responsabilidade, como a culpa exclusiva da vítima, deve a empresa tomar algumas medidas capazes de demonstrar a ausência de culpa subjetiva e suas modalidades, quais sejam: *culpa in eligendo, culpa in vigilando, culpa in omittendo, culpa in custodiendo* e *culpa in contraendo*. Para tanto, algumas medidas como o investimento em recursos de tecnologia da informação compatíveis com o mercado (ex.: técnicas de proteção de banco de dados, firewall etc.), a vigilância mínima sobre os dados trafegados, o uso de recursos como criptografia e, ainda, a transparência e orientação para que os usuários se protejam melhor, são exemplos de medidas capazes de atenuar eventual responsabilidade da empresa perante um juízo.

Avançando na prática

Responsabilidade civil por fraudes bancárias

Descrição da situação-problema

Determinada instituição financeira o contratou como consultor de segurança da informação para sugerir medidas capazes de diminuir os valores gastos com indenizações pagas diante do crescente aumento de fraudes bancárias, praticadas majoritariamente por meio de sua ferramenta Internet Banking. Quais medidas você sugeriria? Qual a culpa da empresa em razão das fraudes? Em sua resposta, você deverá considerar cada um dos tipos ou modalidades de culpa subjetiva e quais medidas podem ser adotadas para demonstrar eventual ausência daquele tipo de culpa.

Lembre-se

São cinco as modalidades de culpa dentro de um contexto de internet e ambiente eletrônico estudas nesta seção. São elas: *culpa in eligendo, culpa in vigilando, culpa in omittendo, culpa in custodiendo* e *culpa in contraendo*.

Resolução da situação-problema

Considerando um cenário de fraude bancária praticada pela internet, temos as seguintes modalidades de culpa que podem ser atribuídas à instituição bancária e as respectivas medidas de contingenciamento, capazes de mitigar eventual responsabilidade pelo dano causado aos clientes:

- *culpa in eligendo*, decorrente da escolha ou opção pelos serviços. Em nosso contexto de fraude bancária, podemos dizer que o banco prestador de serviços em ambiente eletrônico (ex.: *Internet Banking*) terá culpa se houver adquirido recursos informáticos inadequados, ou seja, caso não tenha adotado cuidados razoáveis na escolha de tais recursos, como consultorias especializadas e tecnologias adequadas para proteger seus clientes.

- *culpa in vigilando*, que é a culpa em razão da violação de um dever de vigilância. Em nosso problema, trata-se do dever do banco de realizar uma vigilância mínima sobre as transações efetuadas por seus clientes. Não se trata de uma vigilância sobre todas as operações, o que poderia resultar também em violação à privacidade de seus clientes. Trata-se da vigilância, por exemplo, de transações estranhas e incomuns. Algumas instituições fazem isso, entrando em contato com seus clientes em caso de compras suspeitas realizadas com cartão de crédito pela internet.

- *culpa in omittendo*, ou culpa decorrente da omissão de informações relevantes. Este é um tópico polêmico, tendo em vista uma variação muito grande entre o nível de informação dos próprios usuários. Assim, a omissão deve ser analisada com cautela, limitando-se essencialmente a questões de segurança.

- *culpa in custodiendo*, que trata da culpa pela violação do dever de guarda ou custódia. Trata-se, por exemplo, da responsabilidade do banco em relação à guarda de dados de seus usuários. Deve a instituição garantir a integridade de tais dados adotando medidas proativas, como criptografia, firewalls etc.

- *culpa in contraindo*, modalidade semelhante à *culpa in eligendo*, mas diz respeito à responsabilidade por cumprir com aquilo que foi prometido. Para nosso exemplo, trata-se do dever do banco de ofertar serviços com segurança mínima razoável. Caso não estejam presentes tais requisitos, não deve a instituição contratar com possíveis interessados.

Faça valer a pena

1. Sobre o instituto da Responsabilidade Civil, assinale a alternativa incorreta:

a) A responsabilidade civil é uma obrigação de natureza pessoal e resolve-se em perdas e danos, conforme dispõe o atual Código Civil

em seu artigo 389.

b) O instituto da responsabilidade civil integra o chamado "direito das obrigações" e resulta na obrigação de reparar eventual dano ocasionado.

c) A responsabilidade civil pode ser entendida como verdadeira ferramenta para o restabelecimento de um equilíbrio social. Nesse sentido, aquele que causa um dano tem o dever legal de repará-lo.

d) De acordo com o instituto da responsabilidade civil, quem pratica um ato, ou incorre numa omissão da qual resulte dano, sob hipótese nenhuma deve suportar as consequências do seu procedimento.

e) A responsabilidade civil já se encontrava prevista no Código Civil de 1916.

2. São elementos ou pressupostos da responsabilidade civil, exceto:

a) Ato.

b) Dano.

c) Conduta.

d) Nexo Causal.

e) Culpa.

3. Qual dos pressupostos da responsabilidade civil estudados melhor define o vínculo que liga a conduta ao resultado danoso?

a) Ato.

b) Dano.

c) Conduta.

d) Nexo Causal.

e) Culpa.

Seção 2.4

Responsabilidade civil dos provedores

Diálogo aberto

Na última seção desta Unidade 2, estudamos o instituto da responsabilidade civil no ordenamento jurídico brasileiro e vimos sua importância para as situações ocorridas no ambiente eletrônico. Uma vez definidos os conceitos próprios deste instituto, passaremos para o estudo da situação específica da responsabilidade civil dos provedores de internet.

Para tanto, devemos antes retomar brevemente nossa Situação Geradora de Aprendizagem (SGA): Suponhamos que você foi contratado por uma empresa que possui um website, no qual diariamente são publicados conteúdos relacionados à cultura pop. A empresa deseja desenvolver uma plataforma de rede social para que seus usuários interajam entre si e compartilhem conteúdos diversos. Seu trabalho consiste também em realizar a blindagem jurídica desta nova aplicação, conforme explicado.

Considere a seguinte situação-problema: Uma vez realizado o pré-lançamento da plataforma de rede social, o chamado "beta", sua equipe de TI encontrou, por meio de consulta a um site de buscas, comentários ofensivos de um usuário sobre uma determinada empresa concorrente. Tendo em vista tal situação, o diretor de TI da empresa pediu que você analisasse se a sua empresa poderia ser responsabilizada por tais comentários ofensivos.

Para resolvermos este problema, devemos aprofundar nossos estudos acerca da responsabilidade civil da internet, de modo a analisarmos a questão específica da responsabilidade civil dos provedores. Para tanto, iremos diferenciar os diversos tipos de provedores e o tratamento que cada um recebe da nossa legislação. Igualmente, iremos analisar a responsabilidade destes por certos tipos de condutas, como o *linking*, o *caching* e o uso de metatags. Por fim, estudaremos alguns provedores de serviços cuja responsabilidade causa confusão em nossos Tribunais, como é o caso dos sites de leilão virtual e motores de busca.

Não pode faltar

Antes de adentrarmos à questão específica da reponsabilidade civil dos provedores, é necessário analisarmos as diferentes categorias ou espécies de provedores de internet.

Assimile

"Provedor" é a empresa que presta serviços relacionados ao funcionamento da internet. "Provedor de serviço" é gênero do qual são espécies os provedores de: backbone, de acesso, de correio eletrônico, de conteúdo e de hospedagem (LEONARDI, Marcel. **Responsabilidade Civil dos provedores de serviços de internet**. São Paulo: Juarez de Oliveira, 2005. p. 19).

De maneira sintética, podemos dividir os provedores nas seguintes categorias: **Provedor de *backbone*** é aquele que detém as estruturas de rede, capaz de possibilitar o tráfego de informações; **provedor de acesso** é o fornecedor de serviços que possibilita o acesso de seus usuários à internet; **provedor de conteúdo**, conhecido também como provedor de serviços, é o que disponibiliza e armazena, em seus servidores, informações criadas por terceiros ou por meios próprios; e, por fim, **provedor de hospedagem** é o que permite o armazenamento de sites, blogs, redes sociais etc., com seus textos, imagens, sons e informações em geral.

Conforme o enquadramento do provedor em uma das categorias acima indicadas, ou seja, conforme sua natureza jurídica, diferente será sua responsabilidade civil pelos atos de terceiros ou pelos próprios atos. Primeiramente, iremos tratar das questões referentes aos **provedores de conteúdo/serviços e hospedagem/armazenamento**.

A responsabilidade daquele que coloca na internet conteúdo ilícito é inquestionável, mas a questão é mais delicada e diz respeito à responsabilidade daquele que, embora não coloque na rede a ilegalidade, contribui para que o ilícito seja mais facilmente difundido, como é o caso dos provedores de conteúdo e hospedagem.

Em nosso ordenamento jurídico, especificamente na Lei nº 12.965/2014 do Marco Civil da Internet, ao definir provedor de conteúdo e hospedagem como provedor de aplicação de internet, estabeleceu-se que não cabe a este fiscalizar o teor da mensagem (ex.: fotos, vídeos, mensagens) dos usuários por ser a eles assegurada a liberdade de expressão. De acordo com o artigo 19 do Marco Civil, o provedor de aplicação somente será responsabilizado por danos decorrentes de

atos de terceiros se descumprir ordem judicial específica para tornar indisponível o conteúdo considerado danoso.

Assim, somente a Justiça, mediante provocação do interessado, é que poderá avaliar se determinado conteúdo é prejudicial ou não a outrem. Uma exceção está prevista no artigo 21 do Marco Civil, ao prever que em caso de cenas de nudez ou atos sexuais de caráter privado, o provedor que disponibilizar o conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação sem autorização dos participantes quando, após recebimento de notificação por um destes participantes, deixar de levar e promover, de forma diligente, no âmbito e nos limites técnicos de seus serviços, a indisponibilização do conteúdo. Trata-se de exceção que visa coibir a prática do "*Revenge porn*" ou "pornô de vingança". Reparem que não se trata de ordem judicial, mas sim, de mera notificação do interessado ao provedor.

Exemplificando

A título de exemplificação, vamos considerar uma situação clássica envolvendo a responsabilidade civil dos provedores de aplicação ou de conteúdo e hospedagem: Um usuário, ao sentir-se ofendido pelo conteúdo de páginas em rede social da internet, propõe ação judicial contra o titular daquela aplicação (ex.: Facebook), visando à retirada daquele conteúdo e indenização por eventuais danos morais. Neste caso, aplica-se o artigo 19 do Marco Civil, que consubstancia uma responsabilidade subjetiva, conforme estudamos na seção anterior. Antes da aprovação do Marco Civil, alguns Tribunais aplicavam a teoria do risco, ou responsabilização objetiva, que restou afastada desde então.

Quanto à responsabilidade dos **provedores de acesso** ou conexão, podemos dizer que sua responsabilidade se refere à qualidade com que presta seus serviços, ou seja, em caso de defeito ou vício do serviço de acesso prestado, ele pode ser responsabilizado pelos danos que eventualmente causar. Neste caso, importante salientar que é possível a aplicação do Código de Defesa do Consumidor (CDC), por ser o provedor de acesso um fornecedor de serviços, na acepção jurídica da palavra. Ou seja, caso um usuário sinta-se prejudicado ou experimente algum dano ligado à má-prestação de serviços de conexão, poderá querer indenização, caso comprove estarem presentes os elementos da responsabilidade civil, os quais vimos na seção anterior.

Doutro lado, quanto à responsabilidade desses provedores de conexão e ao conteúdo gerado por terceiros, o Marco Civil da Internet, em seu artigo 18, define que estes não serão responsabilizados por tais danos. Dessa forma, o provedor de

acesso é considerado mero condutor, a exemplo das companhias telefônicas, que não se responsabilizam pelo uso do telefone para a prática de ilícitos.

A responsabilidade civil dos provedores de internet está tratada de uma maneira ampla e geral no Marco Civil da Internet, conforme vimos anteriormente. Porém, existem algumas situações específicas que demandam uma análise um pouco mais detalhada por não estarem tão claras, sobretudo sob o ponto de vista dos nossos julgadores.

Como sabemos, a vítima de um dano pode pleitear a devida reparação por meio dos mecanismos da responsabilidade civil. Existem algumas condutas praticadas na internet que podem ser passíveis de punição e que estão intrinsecamente ligadas à prática de Concorrência Desleal, que estudaremos melhor na Unidade 3, com foco na questão da reponsabilidade civil.

A primeira refere-se à prática do *linking*, que por sua vez consiste em vincular determinado segmento de uma página a outra, acessível por um único clique. O *linking* se torna um problema quando é usado para vincular determinado conteúdo ilícito. Caso determinado site coloque em seu conteúdo um link que hospede um outro conteúdo ilícito, poderia o primeiro ser responsabilizado pelo conteúdo constante no segundo? A princípio, somente poderia ser responsabilizado em caso de descumprimento de ordem judicial específica (art. 19 do Marco Civil) ou caso tenha sido notificado do conteúdo ilícito que envolva nudez (art. 21 do Marco Civil).

A segunda prática se trata do *caching*. Este, por sua vez, pode ocorrer no computador de um usuário por meio de um mecanismo disponível em seus navegadores, que cria um diretório (cache) no qual são armazenados os endereços dos sites mais visitados, ou ainda, caso armazenados nos servidores do provedor de conexão. O problema surge quando o usuário carrega uma página acreditando ser esta a mais atual, mas, na verdade, se trata de versão desatualizada daquela página. Neste caso, a empresa que manteve sua página desatualizada poderá ser responsabilizada pelos danos causados ao usuário.

A terceira, e última, refere-se ao mau uso de metatags. Os metatags são códigos de programação que possuem a função de indicar o assunto tratado no site, facilitando sua catalogação por mecanismos de busca, como Google e Bing. Os problemas surgem a partir da inserção, nos metatags, de palavras que fazem referência ao produto de um concorrente ou marca registrada de terceiro, podendo ser punível a depender da extensão do dano causado.

Ademais, cumpre tecermos algumas considerações sobre aqueles que operam como intermediários na internet e os contornos de suas responsabilidades civil diante de consumidores. Na internet, são encontrados vários tipos de negócios que podem ser tidos como de intermediação. Como vimos, para que seja possível utilizar a internet são necessários vários serviços que, por sua vez, são prestados

pelos denominados provedores de serviços de internet.

Esses provedores são classificados conforme o papel que desempenham, sendo que nosso objetivo é verificar se a intermediação de negócios na internet pode ser enquadrada em uma das espécies de provedores, bem como analisar o nível de responsabilidade que o intermediário deve ter.

Alguns sites têm por atividade permitir a intermediação entre vendedores (fabricantes, produtores, importadores, varejistas, particulares) e compradores, ligando-os. Nesses sites, os vendedores/prestadores cadastram-se e anunciam seus produtos e serviços a serem adquiridos pelos clientes, sendo que a negociação pode ocorrer na própria plataforma do intermediário ou não. Nesta categoria, a remuneração consiste, normalmente, em uma comissão sobre o valor anunciado para o produto, podendo ser, também, por anúncios realizados ou por quantidade de cliques no anúncio do vendedor.

Entendemos que é possível classificar a atividade de intermediação de compras pela internet como provedor de conteúdo. Quanto ao nível de responsabilidade deste, os nossos Tribunais divergem nesta questão. Ao nosso ver, há responsabilidade da empresa intermediária de indenizar, caso sua prestação de serviço seja falha e não garanta ao usuário-comprador a segurança necessária, permitindo a concretização de cadastro em seu site de usuário-vendedor que descumpre com a negociação firmada. Por isso, efetuado o pagamento ao vendedor cadastrado no site da intermediária, e não sendo o produto enviado ao comprador, configura-se ato ilícito e defeito do serviço em desfavor da intermediária, que poderá responder pelos danos suportados pelo comprador.

Outra modalidade controversa refere-se aos motores de busca, por exemplo, o Google.

Reflita

Teriam os motores de busca responsabilidade civil pelo conteúdo que aparece em sua página de resultado de pesquisa? Apesar de não hospedarem o conteúdo, estão contribuindo para sua divulgação, potencializando eventual dano causado a uma vítima.

Após o advento do Marco Civil, podemos facilmente enquadrar os motores de busca na categoria de provedores de conteúdo ou hospedagem, o que afasta sua responsabilidade civil pelo conteúdo divulgado por terceiros. Dessa maneira, caso um usuário encontre um conteúdo ofensivo hospedado na primeira página de busca do Google, ele 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 busca não possui responsabilidade por conteúdos publicados

por terceiros hospedados em outros sites da internet. Por consequência, os sites de busca não têm o dever de monitorar conteúdos que aparecem em seus resultados de pesquisa, sob pena de tal conduta configurar-se censura prévia, limitando, assim, o direito de liberdade de expressão. A título de exemplo, temos alguns casos emblemáticos, como da apresentadora "Xuxa", em que o Superior Tribunal de Justiça decidiu que a empresa Google não era responsável pelos conteúdos e imagens relativas à busca utilizando os termos "Xuxa pedófila" ou por qualquer expressão em que o resultado associasse o nome artístico da apresentadora a alguma prática criminosa.

Pesquise mais

Caso queira explorar mais a questão da responsabilidade civil dos provedores, sugerimos a leitura do artigo "Responsabilidade Civil de Provedores de Conteúdo da Internet", escrito por Thiago Guimarães Moraes. Disponível em: <https://www.ibdcivil.org.br/image/data/revista/volume4/05---rbdcivil-volume-4---responsabilidade-civil-de-provedores-de-conteuodo-da-internet.pdf>. Acesso em: 12 jul. 2016.

Sem medo de errar

Vistos os principais conceitos, vamos resolver nossa situação-problema: Uma vez realizado o pré-lançamento da plataforma de rede social, o chamado "beta", sua equipe de TI encontrou, por meio de consulta a um site de buscas, comentários ofensivos de um usuário sobre uma determinada empresa concorrente. Tendo em vista tal situação, o diretor de TI da empresa pediu que você analisasse se a sua empresa poderia ser responsabilizada por tais comentários ofensivos.

Atenção

A Lei nº 12.965/14 do Marco Civil da Internet, em seu artigo 19, dispõe que o provedor de aplicação de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiro se, após ordem judicial específica, não tomar providências para tornar indisponível o conteúdo considerado infringente.

Ao desenvolver a rede social, foi criada uma ferramenta com a qual é possível que os usuários da aplicação realizem comentários diversos. No caso de tais comentários serem considerados ilícitos ou ofensivos, poderia a empresa titular da aplicação ser responsabilizada por tal conteúdo? Em nosso ordenamento jurídico, especificamente na Lei nº 12.965/2014 do Marco Civil da Internet, ao definir um

provedor de conteúdo e hospedagem como provedor de aplicação de internet, estabeleceu-se que não cabe a este fiscalizar o teor da mensagem (ex.: fotos, vídeos, mensagens) dos usuários por ser a eles assegurada a liberdade de expressão. De acordo com o artigo 19 do Marco Civil, o provedor de aplicação somente será responsabilizado por danos decorrentes de atos de terceiros se descumprir ordem judicial específica para tornar indisponível o conteúdo considerado danoso.

Somente a Justiça, mediante provocação do interessado, é que poderá avaliar se determinado conteúdo é prejudicial ou não a outrem. Uma exceção está prevista no artigo 21 do Marco Civil, ao prever que em caso de cenas de nudez ou atos sexuais de caráter privado, o provedor que disponibilizar o conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade, decorrente da divulgação sem autorização dos participantes quando, após recebimento de notificação por um dos participantes, deixar de levar e promover, de forma diligente, no âmbito e nos limites técnicos de seus serviços, a indisponibilização do conteúdo.

Portanto, poderá a empresa ser responsabilizada civilmente caso deixe de cumprir ordem judicial específica, ou não cumpra eventual notificação em caso de conteúdo íntimo. Cumpre ainda esclarecermos que o site de buscas também não poderá ser responsabilizado nos casos em que pese comentários ofensivos indexados na página de resultado de buscas.

Avançando na prática

Revenge Porn e suas consequências jurídicas

Descrição da situação-problema

Considere que o aplicativo de rede social citado na situação-problema desta seção já esteja em pleno funcionamento. Certo dia, foi recebida pela empresa uma Notificação Extrajudicial de um usuário relatando que outro usuário estaria divulgando um vídeo no qual o usuário notificante praticava sexo com outra pessoa, em local privado. De posse do endereço eletrônico em que o conteúdo está hospedado, você e a equipe de TI localizaram o conteúdo e confirmaram que realmente se trata de cena de nudez e atos sexuais. Para evitar eventual responsabilização civil, como deve a empresa titular da aplicação agir?

Lembre-se

A Lei nº 12.965/14 do Marco Civil da Internet, em seu artigo 21, traz uma exceção à regra geral contida no artigo 19 que define a responsabilidade civil do provedor de aplicação.

Resolução da situação-problema

Conforme o artigo 21 da Lei nº 12.965 de 2014 do Marco Civil da Internet, o provedor de aplicações de internet que disponibilizar 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. Assim, caso a empresa titular da aplicação receba uma Notificação Extrajudicial nos termos do citado artigo 21, deverá indisponibilizar o conteúdo independentemente de ordem judicial específica, com objetivo de evitar eventual responsabilização civil.

Faça você mesmo

As agressões e a divulgação de conteúdos on-line são algo recorrente na internet. Convidamos vocês a assistir ao vídeo, (disponível em: <https://www.youtube.com/watch?v=0bnXni1pLHI>. Acesso em: 19 jul. 2016.), em que a Dra. Gisele Truzzi explica o tema e dá algumas dicas aos usuários. Após o vídeo, sugerimos que seja feita uma lista com os principais tipos de agressões e analisada a responsabilidade do provedor em cada uma das situações, de acordo com o Marco Civil.

Faça valer a pena

1. "Provedor" é a empresa que presta serviços relacionados ao funcionamento da internet. "Provedor de serviço" é gênero do qual são espécies os seguintes provedores, exceto:

a) Backbone.

b) Conteúdo.

c) Telefonia.

d) Hospedagem.

e) Acesso.

2. O provedor que detém as estruturas de rede, capaz de possibilitar o tráfego de informações, é também conhecido como provedor de:

a) Hospedagem.

b) Conteúdo.

c) Correio eletrônico.

d) *Backbone*.

e) Acesso.

3. Sobre a responsabilidade civil do provedor de aplicação, assinale a alternativa incorreta:

a) Conforme a Lei nº 12.965/2014 do Marco Civil da Internet, ao provedor de aplicação não cabe a fiscalização do teor de eventuais mensagens trocadas entre usuários.

b) A fiscalização prévia de conteúdos publicados por usuários não importa nem em censura nem limitação à liberdade de expressão.

c) De acordo com o artigo 19 do Marco Civil, o provedor de aplicação somente será responsabilizado por danos decorrentes de atos de terceiros se descumprir ordem judicial específica para tornar indisponível o conteúdo considerado danoso.

d) Em casos de conteúdos envolvendo cenas de nudez e atos sexuais é desnecessária ordem judicial específica, bastando Notificação Extrajudicial para atrair eventual responsabilidade civil ao provedor de aplicação.

e) A indisponibilização de conteúdos considerados ilícitos deve ser realizada dentro dos limites técnicos do provedor de aplicação.

Referências

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

BITTAR, C. A. **Os direitos da personalidade**. 5. ed. atual. por Eduardo Carlos Bianca Bittar. Rio de Janeiro: Forense Universitária, 2001.

BOBBIO, N. **A era dos direitos**. 19. ed. Trad. de Carlos Nelson Coutinho. Rio de Janeiro: Elsevier, 1992.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 17 jul. 2016.

_____. Lei nº 3.071, de 1º de janeiro de 1916. Código Civil dos Estados Unidos do Brasil (Revogada). **Diário Oficial da União**, Rio de Janeiro, RJ, 5 jan. 1916. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l3071.htm>. Acesso em: 17 jul. 2016.

_____. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, DF, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 17 jul. 2016.

CANOTILHO, J. J. **Direito constitucional e teoria da constituição**. Coimbra: Almedina, 1988.

CASTRO, M. N. A. S. **Honra, imagem, vida privada e intimidade, em colisão com outros direitos**. Rio de Janeiro: Renovar, 2002.

FARIAS, E. P. **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, P. S; PAMPLONA FILHO, R. **Novo curso de direito civil**. 9. ed. São Paulo: Saraiva, 2011. v. 3: Responsabilidade civil.

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

MOLON, Alessandro. **Marco civil da internet**: a garantia de direitos fundamentais do usuário. Disponível em: <http://www.oabrj.org.br/materia-tribuna-do-advogado/18113-marco-civil-da-internet-agarantiade-direitos-fundamentais-do-

usuario>. Acesso em: 30 abr. 2016.

PINHEIRO, P. P. **Direito digital**. São Paulo: Saraiva, 2013.

ROHRMANN, C. A. **Curso de direito virtual**. Belo Horizonte: Del Rey, 2005.

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

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

TRUZZI, G. ***Revenge porn*, difamação, *cyberbullying* e ameaça na internet**. ONG Think Olga. Camapnha MandaPrints. Dra. Gisele Truzzi. Youtube, 8 dez. 2015. Disponível: <https://www.youtube.com/watch?v=0bnXni1pLHI>. Acesso em: 12 jul. 2016.

Propriedade intelectual e nomes de domínio

Convite ao estudo

O surgimento da internet e das novas tecnologias da informação facilitou a distribuição de obras e trabalhos através do meio eletrônico, tais como livros, músicas, fotos, além de programas de computador. Tal fato gerou um cenário no qual a pirataria de obras tornou-se recorrente, para não dizer institucionalizada. O Direito da Propriedade Intelectual apresenta-se como uma das soluções mais efetivas (e antigas) para a proteção dos direitos de autores e inventores sobre suas obras e criações. Nesta unidade, iremos estudar o Direito da Propriedade Intelectual, sobretudo aplicado a situações geradas na internet e no meio digital. Os objetivos específicos desta Unidade 3 referem-se justamente ao estudo das principais formas de proteção da propriedade na internet, como o direito autoral e o registro de marcas, além de conhecer as principais leis que regulam o tema, como a Lei nº 9.609/1998 ("Lei do Software") e a Lei nº 9.610/1998 ("Lei de Direitos Autorais").

Para esta unidade, iremos considerar a seguinte situação geradora de aprendizagem (SGA): Você foi contratado por uma empresa de engenharia para desenvolver um software do tipo CAD (desenho assistido por computador), destinado à criação de modelos tridimensionais de estruturas. A contratação foi realizada verbalmente, não tendo sido redigido nenhum contrato. Finalizado o projeto, a empresa registrou o software junto ao Instituto Nacional da Propriedade Intelectual (INPI). Tal software tornou-se conhecido pelos concorrentes da empresa de engenharia, que o contrataram para desenvolver solução idêntica. Para tanto, você criou uma nova pessoa jurídica para comercializar tal software. Ao tentar registrar o nome de domínio da empresa na internet, você verificou que ele já havia sido comprado por terceiro, que tentou revender o nome de domínio por uma alta quantia. Além disso, a empresa original que registrou o software entrou com uma ação na justiça contra você requerendo danos pela contrafação, ou venda não autorizada do software. Pergunta-se: De quem é a titularidade do software neste caso?

A ação judicial impetrada possui procedência? É possível reaver o nome de domínio registrado por terceiro? Como?

Ao longo das seções desta unidade, iremos tratar sobre o sistema da Propriedade Intelectual no Brasil e suas diferentes formas de proteção. Ainda, iremos ver a questão dos direitos autorais na internet e o impacto das novas tecnologias e novos modelos de negócio para o Direito da Propriedade Intelectual. Iremos analisar a questão das marcas registradas, dos nomes de domínio e da concorrência desleal, além de analisarmos os aspectos gerais da Lei do Software.

Seção 3.1

A propriedade intelectual no meio digital

Diálogo aberto

A SGA desta unidade traz uma situação muito comum no mercado de trabalho, que é a contratação específica para desenvolvimento de soluções de software. Nestes casos, a questão da titularidade do programa de computador poderá ser controvertida, caso as regras da contratação não sejam ajustadas de maneira muito clara, desde o início dos trabalhos.

Para esta seção, temos a seguinte situação-problema: Considere novamente o cenário proposto na SGA desta unidade, na qual você foi contratado para desenvolver um software de CAD para uma empresa de engenharia. Uma vez finalizado o programa de computador, você, como profissional cauteloso que é, deseja protegê-lo contra eventuais usos não autorizados e pirataria. Dentre as diversas formas de proteção da Propriedade Intelectual (patentes, marcas, direitos autorais etc.), qual a adequada para proteção do programa de computador?

Para resolvermos este problema, devemos abordar, de maneira geral, o conceito de Propriedade Intelectual, sua evolução história e seus principais aspectos econômicos. Iremos, ainda, analisar cada uma das diferentes formas de proteção jurídica da propriedade intelectual. Estudaremos os conceitos relacionados a direitos autorais, direitos conexos, desenhos industriais, marcas registradas, patentes etc., categorizando-os em Propriedade Intelectual, Direitos Autorais, Propriedade Industrial e Direitos *sui generis*, indicando também os principais dispositivos legais.

Não pode faltar

A internet e o mundo virtual têm causado profundos desafios para o Direito da Propriedade Intelectual. Os motivos são simples: a facilidade de localização da propriedade intelectual no mundo virtual, a perfeição e a rapidez das cópias, além de seu baixo custo (que muitas vezes se aproxima de quase nada). Todavia, antes de adentrarmos no estudo da fragilidade e necessidade de proteção de dados e informações em formato digital, cumpre tecermos algumas considerações sobre a

Propriedade Intelectual em si e sua consequente proteção jurídica, particularmente no território brasileiro.

Então, o que é Propriedade Intelectual? Você provavelmente sabe a resposta dessa questão. Sabemos que o inventor de uma máquina, o autor de um livro, ou o compositor de uma canção é, geralmente, o "proprietário" de sua obra. Por essa razão, não podemos simplesmente sair copiando sua obra quando bem entendermos, ou ainda, comprarmos uma cópia do trabalho sem considerar o recolhimento dos respectivos direitos autorais. Todas as vezes que compramos esses produtos protegidos, uma parte do valor pago é revertido ao titular daquela obra ou invento, como forma de recompensa pelo tempo, dinheiro, esforço e conhecimentos investidos na criação intelectual.

Assimile

Propriedade Intelectual é a área do Direito que, por meio de leis e tratados internacionais, garante a inventores, autores, ou responsáveis por qualquer produção do intelecto - seja nos domínios industrial, científico, literário ou artístico - o direito de obter, por um determinado período de tempo, proteção e recompensa pela própria criação.

Cada país, independentemente de tratados internacionais, pode legislar sobre a propriedade intelectual em seu território nacional. Especificamente no Brasil, temos as seguintes formas de proteção jurídica da propriedade intelectual:

- Direito de Autor, que protege obras intelectuais e artísticas, bem como programas de computador.
- Direitos Conexos, que protege as interpretações sobre as obras artísticas.
- Marcas registradas, que protege principalmente denominações comerciais.
- Desenhos industriais, que protege o design de determinadas obras.
- Patentes, que protegem invenções e modelos de utilidade.
- As Indicações Geográficas, que protegem produtos e serviços originados de determinada região (ex.: queijos e vinhos).
- Proteção de Novas Variedades de Plantas (Cultivares), que protege as plantas geneticamente alteradas.
- Proteção da Topografia de Circuito Integrado, que protege o desenho de circuitos integrados.

Para entendermos melhor o conceito de "propriedade intelectual", temos que, antes, considerar o significado do termo "propriedade", isoladamente. O direito de propriedade é garantido no Brasil por força do disposto na Constituição Federal de 1988 (Art. 5º, inciso XXII) e do Código Civil de 2002 (Art. 1.228). Este último, por sua vez, seguindo a tradição do Código Civil de 1916, não define o conceito de direito de propriedade, apenas enumera os direitos do proprietário, que são os de usar, gozar, dispor, rever e reivindicar a coisa de quem quer que a possua ou detenha injustamente. Ou seja, em sua maioria, os diferentes tipos de propriedade têm em comum o fato de que seu titular é livre para usá-la e impedir alguém de utilizá-la, contanto que o uso não seja contrário à lei e não interfira no direito de terceiros.

Historicamente, podemos dizer que a evolução do direito de propriedade aponta uma primeira fase como sendo um direito voltado, principalmente, para os bens corpóreos, especialmente os bens imóveis. Foi somente há, aproximadamente, 300 anos que surgiu a proteção específica do direito de propriedade intelectual, com a edição das primeiras leis de copyright na Grã-Bretanha. Interessante notar que as primeiras discussões acerca do direito de propriedade intelectual surgiram após o advento da imprensa mecânica.

Curioso notar que os livros dos autores ingleses estavam sendo copiados de forma "industrial", em larga escala, e sendo revendidos em suas colônias, especialmente nos Estados Unidos, sem que os autores recebessem o devido valor pela comercialização de suas obras. Isso fez com que o parlamento inglês, no ano de 1710, aprovasse o chamado Statute of Anne. Esta Lei, por sua vez, conferia aos autores britânicos o direito exclusivo sobre suas obras por um prazo de 14 anos, renováveis por um período de mais 14 anos.

Quantos às patentes, foi em Veneza, na época uma cidade-estado dedicada ao comércio, que surgiu a primeira lei que remete ao nosso atual sistema de proteção patentária. Com origem no senado veneziano, em 1474, a "Lei de Veneza" conferia ao inventor privilégio ou monopólio sobre sua invenção pelo prazo de dez anos.

A evolução que vimos acima, muito brevemente, demonstra que a proteção jurídica tende a ser tão mais elaborada para a propriedade conforme a época e conforme o tipo de propriedade de maior importância prática e econômica na vida das pessoas. Atualmente, vemos um crescimento da importância da propriedade intelectual ou imaterial, seja através da indústria do entretenimento, que demanda proteção para os programas de computador, para as músicas, filmes e jogos digitais; seja por meio da indústria, que demanda proteção patentária para invenções e modelos de utilidade.

Observa-se, ainda, o aumento da importância da informação na economia, presente não só em obras protegidas, como também em banco de dados. A intangibilidade trazida pela Sociedade Digital impõe um grande desafio para todos

os envolvidos, desde os criadores das obras até os operadores do Direito. A cada dia, presenciamos a criação de novos modelos de negócios que desafiam o entendimento do Judiciário acerca da implementação de soluções já consolidadas pelos Tribunais.

Assim, após a concessão do direito de propriedade intelectual, esse instrumento oferece ao detentor do direito a possibilidade de inserir seu produto/serviço no mercado, aumentando seu poder de negociação e, ainda, resguardando-o contra práticas concorrenciais desleais por parte dos competidores. Além de resguardar o esforço dos autores e inventores, o sistema de propriedade intelectual tem por objetivo, também, corrigir desequilíbrios econômicos e criar incentivos para a produção de novas obras e invenções. Inclusive, esse aspecto "econômico" da propriedade intelectual é extremamente marcante.

Na verdade, a proteção da propriedade intelectual assemelha-se muito a uma espécie de monopólio sobre a exploração da obra criada. Como dissemos, esse monopólio é justificado pela necessidade de recompensar o autor ou inventor pelo esforço despendido na criação daquele invento. Contextualizando esse cenário, seria uma forma de resguardar todos os investimentos, por exemplo, aportados num setor de pesquisa e desenvolvimento de uma grande empresa. Trata-se de verdadeira forma de incentivo à criação de novas tecnologias e novas produções científico-literárias.

Reflita

Neste estágio, cumpre refletirmos sobre a necessidade do direito de Propriedade Intelectual para corrigir desequilíbrios econômicos. Será que a propriedade intelectual poderia ser substituída por outros sistemas de incentivos, como o financiamento privado? Será que a garantia patentária para medicamentos beneficia a sociedade como um todo, ou protege apenas os grandes laboratórios farmacêuticos?

Passamos agora para um breve estudo das formas de adaptação que o direito de propriedade vive em relação à proteção dos bens intangíveis. Como sabemos, a propriedade intelectual decorre diretamente da capacidade inventiva ou criadora do intelecto humano (conhecimento, tecnologia e saberes) de seus criadores. Em geral, entende-se que o Sistema de Propriedade Intelectual compreende direitos relativos a Direitos de Autor e Conexos, Propriedade Industrial e Direitos *Sui Generis*.

Os **Direitos de Autor e Conexos** são aqueles concedidos aos autores de obras intelectuais, expressas por qualquer meio ou fixadas em quaisquer suportes. Estes direitos incluem: obras literárias, artísticas e científicas (direitos de autor); interpretações artísticas e execuções, fonogramas e transmissões por radiodifusão

(direitos conexos). São eminentemente protegidas pela Lei nº 9.610/1998, conhecida como "Lei de Direitos Autorais". Inclui, ainda, os Programas de Computador, conforme disposto no artigo 1º da Lei nº 9.609/1998, a chamada " Lei do Software", a qual será analisada de maneira mais detalhada na Seção 3.4.

Por sua vez, a **Propriedade Industrial** refere-se aos direitos concedidos ao titular de tecnologias industriais e marcas, com o objetivo principal de promover a criatividade em razão da proteção, disseminação e aplicação industrial de seus resultados. O principal dispositivo legal que protege essa categoria é a Lei nº 9.279 de 1996, conhecida como "Lei da Propriedade Industrial". Temos, nessa categoria, as seguintes forma de proteção:

- Patentes, que protegem invenções ou modelos de utilidade (Art. 6º da Lei nº 9.279/1996).
- Desenhos Industriais, que a forma plástica ornamental de um objeto ou o conjunto ornamental de linhas e cores que possa ser aplicado a um produto, proporcionando resultado visual novo e original na sua configuração externa e que possa servir de tipo de fabricação industrial (Art. 94 da Lei 9.279/96).
- Marcas, que são todos os sinais distintivos e visualmente perceptíveis (Art. 122 da Lei nº 9.279/1996).
- Indicações Geográficas, que se referem ao reconhecimento de um determinado produto ou serviço proveniente de uma determinada área geográfica (Art. 176 da Lei nº 9.279/1996).

Interessante notar que a Lei de Propriedade Industrial ainda coíbe práticas de concorrência desleal, que, de maneira resumida, são aquelas práticas de mercado consideradas predatórias e que visam desviar a clientela do concorrente de maneira ilícita ou desleal ou, ainda, induzir consumidores a erros de maneira propositada.

Exemplificando

Um bom exemplo de prática de concorrência, muito comum no mercado de Tecnologia da Informação, refere-se ao vazamento de dados confidenciais. Quando um empregado se desliga de uma empresa e resolve abrir uma nova, ou mesmo, ir para uma empresa concorrente, caso leve consigo segredos comerciais ou industriais, como o código-fonte de um programa de computador, de titularidade da ex-empregadora ou ex-contratante, está a cometer crime de concorrência desleal conforme previsto no artigo 195 da Lei nº 9.279/1996.

Por fim, temos os **Direitos *sui generis***, que integram o escopo da propriedade intelectual, mas que não abrangem direito de autor nem propriedade industrial. São exemplos:

- Proteção de Novas Variedades de Plantas ou Cultivares, que se refere à proteção do aperfeiçoamento de variedades de plantas a fim de incentivar as atividades de criadores e desenvolvedores de novas variedades dessas plantas;
- Topografia de Circuito Integrado, que se refere a uma série de imagens relacionadas à configuração tridimensional das camadas que compõem um circuito integrado e na qual cada imagem represente, no todo ou em parte, a disposição geométrica ou arranjo da superfície do circuito integrado em qualquer estágio de sua concepção ou manufatura.

Para facilitar o entendimento relativo às diferentes formas de Proteção da Propriedade Intelectual e os tipos de criações que cada uma delas resguarda, recomendamos que seja consultada a Tabela 3.1:

Tabela 3.1 | Formas de proteção da propriedade intelectual

Regime de proteção da PI	Exemplos
Direito de Autor	Obras intelectuais e artísticas, além de Programas de Computador
Direitos Conexos	Interpretações artísticas
Marcas	Denominações Comerciais
Patentes	Invenções e Modelos de Utilidade
Indicações Geográficas	Produtos de determinada área geográfica (ex.: queijos e vinhos)
Desenho Industrial	Embalagem
Proteção de novas variedades de plantas	Plantas geneticamente modificadas
Topografia de Circuito Integrado	Desenho do Circuito Integrado

Fonte: elaborada pelo autor.

Pesquise mais

Para saber mais a respeito do impacto da tecnologia digital sobre o domínio da propriedade intelectual, sugerimos a leitura do artigo **Propriedade Intelectual e o Mundo Digital**, de autoria do Professor Aires Rover. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/publica%C3%A7%C3%A3o-propriedade-intelectual-e-o-mundo-digital>. Acesso em: 21 ago. 2016.

Sem medo de errar

Introduzidos os conceitos básicos sobre o Direito da Propriedade Intelectual, vamos retomar nossa situação-problema (SP)? Considere novamente o cenário proposto na SGA desta unidade, na qual você foi contratado para desenvolver um software de CAD para uma empresa de engenharia. Uma vez finalizado o programa, você, como profissional cauteloso que é, deseja proteger seu programa de computador contra eventuais usos não autorizados e pirataria. Dentre as diversas formas de proteção da Propriedade Intelectual (patentes, marcas, direitos autorais etc.), qual a adequada para proteção do programa de computador?

Atenção

Propriedade Intelectual é a área do Direito que, por meio de leis e tratados internacionais, garante a inventores, autores, ou responsáveis por qualquer produção do intelecto - seja nos domínios industrial, científico, literário ou artístico - o direito de obter, por um determinado período de tempo, proteção e recompensa pela própria criação. Esta divide-se em Direitos Autorais, Propriedade Industrial e Direitos *Sui Generis*.

Como vimos ao longo desta seção, cada país, independentemente de tratados internacionais, pode legislar sobre a propriedade intelectual em seu território nacional. Especificamente no Brasil, temos as seguintes formas de proteção jurídica da propriedade intelectual: Direitos Autorais e Conexos, Patentes, Desenhos Industriais, Marcas Registradas, Indicações Geográficas, Cultivares e Proteção da Topografia de Circuitos Integrados. Os Direitos de Autor e Conexos são aqueles concedidos aos autores de obras intelectuais, expressas por qualquer meio ou fixadas em quaisquer suportes. Estes direitos incluem: obras literárias, artísticas e científicas (direitos de autor); interpretações artísticas e execuções, fonogramas e transmissões por radiodifusão (direitos conexos). São eminentemente protegidas pela Lei nº 9.610/1998, conhecida como "Lei de Direitos Autorais". Inclui ainda os Programas de Computador, conforme disposto no artigo 1º da Lei nº 9.609/1998, a chamada " Lei do Software". Assim, temos que o software de CAD a ser desenvolvido para a empresa de engenharia será protegido por Direitos Autorais.

Avançando na prática

Eureca!

Descrição da situação-problema

Você, na condição de desenvolvedor atuante na indústria de entretenimento,

teve uma ideia brilhante para um jogo digital a ser comercializado nas principais lojas de aplicativos de celular. Todavia, tal jogo demanda o emprego de recursos dos quais você não tem condição de dispor, em razão dos elevados custos financeiros, tais como, mão de obra e marketing. Assim, você leva a ideia a uma grande empresa de desenvolvimento de jogos digitais. Após conversas iniciais, você apresenta sua ideia, que é recebida com muito entusiasmo pelos executivos, que pedem para você aguardar, pois estariam passando por algumas reestruturações internas. Um mês após essas conversas, a empresa lança no mercado um jogo idêntico àquele que você inicialmente idealizou. Pergunta-se: Seria possível propor uma demanda judicial fundamentada, acusando a empresa de violação da sua propriedade intelectual?

Lembre-se

As formas de proteção jurídica da propriedade intelectual resguardam a expressão de uma ideia, e não a ideia pura e simples.

Resolução da situação-problema

Conforme vimos ao longo da seção, o Direito da Propriedade Intelectual é um mecanismo importante para a proteção dos bens imateriais, além de necessário para corrigir eventuais falhas de mercado. Podemos dividir tal sistema em três: Direitos Autorais e Conexos; Propriedade Industrial; e Direitos *sui generis*. Todavia, todos eles possuem uma semelhança, que é justamente a necessidade de transposição das ideias para o "mundo real". Ou seja, as ideias, consideradas de maneira isolada, não possuem proteção pela propriedade intelectual. Apenas a expressão dessas ideias pode ser resguardada juridicamente. Destarte, eventual demanda judicial, tendo como base a violação de propriedade intelectual, seria inviável para proteger o autor de uma ideia. Este ramo do direito requer, necessariamente, a transposição da ideia para o "mundo real".

Faça você mesmo

Para conhecer mais sobre as formas de proteção da propriedade intelectual, convidamos você a acessar o site do Instituto Nacional da Propriedade Intelectual (INPI). Lá, você poderá aprofundar seus conhecimentos sobre cada uma das formas de proteção da PI, bem como o procedimento para registro de cada uma delas. Disponível em: <http://www.inpi.gov.br/>. Acesso em: 22 ago. 2016.

Faça valer a pena

1. Assinale a alternativa que NÃO apresenta uma forma de proteção da propriedade intelectual adotada no território brasileiro:

a) Patentes.

b) Direitos Autorais.

c) Direitos Conexos.

d) Copyright.

e) Indicações geográficas.

2. Os programas de computador são protegidos por qual das formas de proteção à Propriedade Intelectual, abaixo elencadas?

a) Cultivares.

b) Direitos Autorais.

c) Direitos Conexos.

d) Marcas Registradas.

e) Indicações geográficas.

3. Considere as seguintes assertivas:

I – O direito de propriedade é garantido no Brasil por força do disposto na Constituição Federal de 1988 e do Código Civil de 2002. Este último, por sua vez, seguindo a tradição do Código Civil de 1916, não define o conceito de direito de propriedade, apenas enumera os direitos do proprietário.

II – Historicamente, podemos dizer que a evolução do direito de propriedade aponta uma primeira fase como sendo um direito voltado, principalmente, para os bens incorpóreos.

III – A primeira lei que veio a tratar especificamente sobre a proteção de obras artísticas surgiu na Inglaterra, há aproximadamente 300 anos.

Estão corretas as afirmativas:

a) I, apenas.

b) I e II.

c) II, apenas.

d) I e IIII.

e) III, apenas.

Seção 3.2

Conflitos envolvendo nomes de domínio

Diálogo aberto

Na Seção 3.1, estudamos, de maneira mais ampla, os conceitos básicos ligados ao Direito de Propriedade Intelectual, suas formas de proteção, evolução histórica, aspectos econômicos, entre outras coisas. Nesta seção, iremos nos aprofundar na questão relacionada à violação do direito de uso de marca, especificamente quanto ao uso de marcas registradas como nomes de domínio na internet.

Retomando nossa SGA, temos que você foi contratado por uma empresa de engenharia para desenvolver um software do tipo CAD, destinado à criação de modelos tridimensionais de estruturas. Para tanto, você criou, em nossa situação-problema anterior, uma nova pessoa jurídica para comercializar tal software. Ao tentar registrar o nome de domínio da empresa na internet, você verificou que ele já havia sido comprado por terceiro, que tentou revendê-lo por uma alta quantia. Neste ponto, você já deve imaginar qual será nossa próxima situação-problema, certo?

Consideremos a seguinte situação-problema: Ao tentar registrar o nome comercial da sua empresa como nome de domínio na internet, você verificou que ele já havia sido comprado por terceiro. Ao acessar o endereço específico, você percebeu que não constava nenhum tipo de conteúdo, ou seja, a página estava literalmente "em branco". Tendo em vista tal situação, você contatou o titular do nome de domínio, que disse que transferiria a titularidade em troca do pagamento de uma alta quantia em dinheiro. Considerando que você deseja ter a titularidade do nome de domínio tanto com a terminação ".com" quanto com a terminação ".br", como você resolveria a questão, sem ter que pagar a quantia pedida pelo atual titular?

Para resolvermos essa questão, iremos estudar o conceito de nome de domínio, o funcionamento do protocolo TCP/IP, os mecanismos e órgãos responsáveis pelos registros dos nomes de domínio, as formas de solução de conflitos, especialmente envolvendo nomes empresariais e marcas registradas.

Não pode faltar

Uma das várias questões jurídicas que surgiram com o advento do uso comercial da internet relaciona-se justamente com a atribuição de nomes para os sítios eletrônicos, devido a um potencial conflito com marcas registradas ou nomes de figuras públicas e famosas.

No final da década de 1960, profissionais da área de engenharia se propuseram a criar protocolos (padrões) que permitissem que computadores, conectados entre si, "falassem uma mesma língua". Esse conjunto de protocolos recebeu o nome de TCP/IP. Você se lembra que na Unidade 1 falamos que a comunicação pela internet é feita por um processo baseado na comutação de dados? Justamente em razão do aumento de volume de dados trocados, foi necessária a adoção de um padrão, até hoje utilizado, para que a rede pudesse crescer da forma mais confiável possível.

Igualmente, sabemos que cada computador e cada sítio eletrônico estão associados a um único endereço, o chamado "endereço IP", que é utilizado pela localização. Atualmente, a versão mais utilizada do protocolo TCP/IP é a quarta versão, ou seja, os números IP são formados por 32 bits, a sua numeração, que é de 0 a 255, resulta em endereços exclusivamente numéricos, com quatro números de 0 a 255, separados por pontos. (ex.: 00.000.000.000). Entretanto, estamos em uma fase de transição da versão quatro (IPv4) para a versão seis (IPv6), sendo os números formados por 128 bits, ou seja, oito grupos de 16 bits, separados por dois pontos (":")", escritos com dígitos hexadecimais (0-F).

Faça você mesmo

Para ativar o protocolo IPv6 em seu computador, ou mesmo verificar se ele está funcionando corretamente, acesse o site IPv6.br. Disponível em: <http://ipv6.br/post/ative-e-use-o-ipv6/>. Acesso em: 22 ago. 2016.

Os endereços numéricos, ou mesmo alfanuméricos, são difíceis de serem utilizados pelas pessoas e empresas, uma vez que a memorização dos números que compõem o endereço eletrônico normalmente não remeteria a nenhum nome ou marca conhecida (ROHRMANN, 2005, p. 199).

Tendo em vista tal dificuldade, criou-se o sistema de nomes de domínio, que busca justamente facilitar a tarefa de endereçamento e localização dos computadores na rede mundial. Assim, em vez de localizar uma página da rede por meio de uma sequência de números, utilizamos nomes do tipo "www.empresaZ.com.br".

Assimile

O que é um nome de domínio? É um nome que serve para localizar e identificar conjuntos de computadores e serviços na internet. O nome de domínio foi concebido com o objetivo de facilitar a memorização desses endereços, pois sem ele, teríamos que memorizar uma sequência grande de números, e dar flexibilidade para que o operador desses serviços altere sua infraestrutura com maior agilidade. Disponível em: <https://registro.br/ajuda.html?secao=novosDominios>. Acesso em: 23 ago. 2016.

Em âmbito brasileiro, os registros de nomes de domínio são feitos no site <www.registro.br>, sendo que o Registro.br é o ente responsável pelo registro e pela manutenção dos nomes de domínio com a extensão ".br". Dessa forma, o interessado ao registrar um nome de domínio na internet, eventualmente, independentemente da intenção, poderá registrar um nome que represente uma marca, um nome pessoal ou nome empresarial etc., cuja titularidade pode não possuir. Isto porque o registro de domínios de sítios eletrônicos é feito por meio do sistema "*first come, first served*", ou seja, "primeiro a chegar pode registrar", não sendo necessário qualquer tipo de comprovação de titularidade da marca ou nome empresarial, por exemplo (TEIXEIRA, 2015, p. 347).

O problema surge, justamente, quando domínios conflitantes com marcas registradas começam a ser registrados por terceiros, que não os legítimos titulares daquela marca. Outra situação problemática ocorre quando se registra um nome de domínio que, embora não seja idêntico ao nome da marca, de certa forma induz o consumidor a erro quanto ao verdadeiro titular do website, configurando-se verdadeira prática de concorrência desleal. Como vimos na Seção 2.4, algumas condutas praticadas pela internet configuram crime de concorrência desleal, sendo, inclusive, indenizáveis em âmbito judicial. Vamos recordá-las? Nesta categoria temos o *linking*, o *caching* e o *metatagging*.

Sobre a hipótese de registro de nome de domínio contendo marca registrada, ou que induza o consumidor a erro, como resolver eventuais conflitos?

Inicialmente, vamos tratar dos nomes de domínio registrados internacionalmente (ex.: ".com"), por cuidar da fonte mais importante de controvérsias, tendo em vista a possibilidade de qualquer pessoa, ao redor do mundo, vir a registrar, pela internet, um domínio ".com". Uma vez que qualquer pessoa pode registrar um domínio desse tipo, é comum que o registro feito por um nacional de um país conflite com marca registrada em outro país.

Neste cenário, a ICANN (Internet Corporation for Assigned Names and

Numbers), 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 (Uniform Dispute Resolution Policy – UDRP), que se apresenta, inclusive, 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).

As decisões arbitrais são, normalmente, favoráveis aos titulares das marcas registradas, no sentido de evitar 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 ".br", adere automaticamente a esse sistema, por força do contrato firmado com a entidade registradora, o "registro.br". Os procedimentos do SACI-Adm limitam-se ao cancelamento e transferência do domínio em disputa, sendo que qualquer pedido de indenização deverá ser levado ao Poder Judiciário.

No segundo caso, temos que o Poder Judiciário também possui competência para resolver conflitos envolvendo nomes de domínio, sendo, inclusive, possível requerer indenização a título de danos morais e materiais em razão do uso indevido da marca, por exemplo.

Reflita

Considerando as formas de resolução de conflitos envolvendo nomes de domínio, especificamente aqueles com a terminação ".br", quais sejam, entre a via arbitral e a judicial, qual você consideraria a mais adequada? Para responder tal questionamento, temos que ponderar as vantagens e desvantagens de ambas. A via arbitral é mais rápida, mas a via judicial possibilita pleitear indenização pelo uso indevido da marca ou nome comercial, por exemplo.

É importante notar que, em todos os casos, seja pela via arbitral, administrativa ou judicial, deve a parte que iniciou o processo demonstrar a "má-fé" no uso do domínio.

Exemplificando

A má-fé pode ser demonstrada de várias maneiras, por exemplo, quando o titular do domínio cobra da empresa detentora da marca a transferência do nome de domínio registrado. Neste caso, temos que o único objetivo da pessoa que o registrou foi revendê-lo através de uma "chantagem".

Quanto 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 se se referir à pessoa pública ou famosa. Trata-se de proteção dos direitos da personalidade dentro da sistemática do Código Civil Brasileiro, especificamente em seus artigos 16 a 19. Assim, os nomes das pessoas naturais são protegidos pelos direitos da personalidade.

Assim, nos casos em que alguém tente fazer o registro de um nome de domínio contendo o nome de terceiro, a princípio, o 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, 2005, p. 212).

A boa-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*". Nesse sentido, aquele que requerer o registro de um nome de domínio que desrespeite a legislação em vigor, que induza terceiros a erro, que seja inviável e viole direitos de terceiros causando enriquecimento ilícito ou prejudicando o consumidor, que represente conceitos predefinidos na internet, que possuam palavras de baixo calão ou abusivas e que façam referência a siglas de Estado e ministérios, é vedado pela norma vigente.

Pesquise mais

Para saber mais sobre os problemas relacionados à transição da versão 4 do protocolo TCP/IP para sua versão 6, sobretudo a questão do

anonimato provocado e a responsabilidade civil dos provedores de conexão, recomendamos a leitura do artigo de FARAH, Rafael Mott. IP NAT: a responsabilidade dos provedores de conexão. Disponível em:<http://pppadvogados.com.br/publicacoes/ppp-news-autor-convidado-3>. Acesso em: 23 ago. 2016.

Sem medo de errar

Ao tentar registrar o nome comercial da sua empresa como nome de domínio na internet, você verificou que ele já havia sido comprado por terceiro. Ao acessar o endereço específico, você percebeu que não constava nenhum tipo de conteúdo, ou seja, a página estava literalmente "em branco". Tendo em vista tal situação, você contatou o titular do nome de domínio, que disse que transferiria a titularidade em troca do pagamento de uma alta quantia em dinheiro. Considerando que você deseja ter a titularidade do nome de domínio, tanto com a terminação ".com" quanto com a terminação ".br", como você resolveria a questão, sem ter que pagar a quantia pedida pelo atual titular?

Atenção

Em âmbito brasileiro, os registros de nome de domínio são feitos no site <www.registro.br>, sendo que o Registro.br é o ente responsável pelo registro e pela manutenção dos nomes de domínio com a extensão ".br". Dessa forma, o interessado, ao registrar um nome de domínio na internet, eventualmente, independentemente da intenção, poderá registrar um nome que represente uma marca, um nome pessoal ou nome empresarial etc., cuja titularidade pode não possuir. Trata-se do sistema "*first come, first served*".

Considerando que, o atual titular do nome de domínio que você deseja registrar para sua empresa não possui marca registrada com tal nome, e também não possui nenhum tipo de vínculo com tal nome, é possível cogitarmos que ele está atuando com verdadeira má-fé, que, por sua vez, é um requisito necessário para um procedimento de transferência de nome de domínio bem-sucedida. No tocante ao domínio ".com", temos que a 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 UDRP, que apresenta-se, inclusive, 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 OMPI. Assim, devemos recorrer a tal mecanismo para resolver o conflito imposto.

Do outro lado, em se tratando do domínio ".br", os conflitos podem ser resolvidos tanto pela via administrativa quanto pela via judicial. No primeiro caso, é necessário recorrermos ao SACI-Adm. Igualmente, podemos recorrer ao Poder Judiciário, que também possui competência para resolver conflitos envolvendo nomes de domínio, sendo, inclusive, possível requerer indenização a título de danos morais e materiais em razão do uso indevido do nome empresarial, por exemplo.

Avançando na prática

Registro de Nome de Domínio

Descrição da situação-problema

Você, na condição de proprietário de uma empresa responsável pelo registro de nomes de domínio junto ao registro.br, foi contratado para registrar um domínio na internet, no qual constará o site oficial de um cantor. Ao tentar registrar o domínio, você verificou que ele já estava registrado em nome de outra pessoa, também com o mesmo nome. Neste endereço eletrônico, o titular do domínio mantinha um blog de culinária. Neste cenário, é possível a instauração de um procedimento arbitral ou judicial para transferência do nome de domínio?

Lembre-se

Os nomes das pessoas naturais são protegidos pelos direitos da personalidade dentro da sistemática do Código Civil Brasileiro, especificamente em seus artigos 16 a 19.

Resolução da situação-problema

Quanto 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 no que concerne à pessoa pública ou famosa. 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, o terceiro tem direito de cancelar ou reaver o registro. A exceção reside justamente nos casos de homônimos. Dessa maneira, o uso do nome de domínio com boa-fé, não seria viável a instauração de procedimento arbitral ou judicial para transferência de nome de domínio, pois a possibilidade de perda da demanda é quase certa.

Faça você mesmo

Para conhecer melhor o sistema SACI-Adm e fixar os conceitos trazidos nesta seção, acesse o endereço eletrônico e leia as regras para resolução de conflitos entre nomes de domínio no Brasil. Disponível em: <https://registro.br/dominio/saci-adm-regulamento.html>. Acesso em: 23 ago. 2016.

Faça valer a pena

1. São características da versão 6 do protocolo TCP/IP (IPv6), exceto:

a) Possui endereçamento alfanumérico de 32 bits.

b) Possui endereçamento alfanumérico de 128 bits.

c) Seus números são escritos com dígitos hexadecimais.

d) Seus números são separados por dois pontos (":").

e) Os números são formados por oito grupos de 16 bits cada.

2. Considere as afirmativas a seguir:

I – Em âmbito brasileiro, os registros de nome de domínio são feitos no site <www.registro.br>, sendo que o Registro.br é o ente responsável pelo registro e pela manutenção dos nomes de domínio com a extensão ".br".

II – Um interessado, para registrar um nome de domínio que represente uma marca, um nome pessoal ou nome empresarial, deve comprovar sua titularidade.

III – O registro de domínios de sítios eletrônicos é feito por meio do sistema "*first come, first served*", ou seja, "primeiro a chegar pode registrar", não sendo necessário qualquer tipo de comprovação de titularidade da marca ou nome empresarial.

Estão corretas as afirmativas:

a) I, apenas.

b) I e II.

c) I e III.

d) II e III.

e) II, apenas.

3. O registro de um nome de domínio que, embora não seja idêntico ao nome de uma marca, mas que de certa forma induz o consumidor a erro quanto ao verdadeiro titular do website, pode configurar:

a) Violação de marca.

b) Violação de direito de autor.

c) Pirataria de software.

d) Prática de concorrência desleal.

e) Violação de patente.

Seção 3.3

Direito de autor e novas tecnologias

Diálogo aberto

Ao longo desta Unidade 3, vimos conceitos básicos ligados ao Direito da Propriedade Intelectual, sendo que, na Seção 3.1, vimos as diferentes formas de proteção dos bens imateriais, a evolução histórica do direito de propriedade, entre outros assuntos. Por sua vez, na Seção 3.2, aprofundamos nossos conhecimentos nas questões relativas aos nomes de domínio, sua relação com a Propriedade Intelectual, especificamente com as marcas registradas e concorrência desleal. Estudamos, também, os mecanismos de resolução de conflitos envolvendo nomes de domínio, tanto em âmbito nacional quanto internacional. Nesta seção, exploraremos questões ligadas a outra forma de proteção da propriedade intelectual, no caso, os Direitos Autorais. Qual a importância dos Direitos Autorais na Sociedade da Informação? Quais os desafios impostos pelas novas tecnologias?

Para responder essas e outras perguntas, precisamos retomar nossa situação geradora de aprendizagem (SGA): você foi contratado por uma empresa de engenharia para desenvolver um software do tipo CAD (desenho assistido por computador), destinado à criação de modelos tridimensionais de estruturas. Finalizado o projeto, a empresa registrou o software junto ao Instituto Nacional da Propriedade Intelectual (INPI).

Para esta seção, considere a seguinte situação-problema: Suponha que, após finalizado, o software encomendado pela empresa é distribuído anonimamente na internet. A partir dessa distribuição é criada uma cópia pirata em que o nome de outra pessoa, e não o seu, aparece como criador daquele programa. Você, como autor, pode vindicar algum direito sobre aquela obra?

Para resolver essa questão, iremos aprofundar nossos conhecimentos sobre os direitos autorais, realizando uma comparação entre este sistema e o copyright. Também, iremos diferenciar direitos morais de direitos patrimoniais e, por fim, analisaremos o impacto e consequências das novas tecnologias sobre o Direito de Autor.

Não pode faltar

As questões relacionadas ao direito de autor envolvem grande parte das discussões jurídicas que se referem ao Direito Eletrônico. Isto porque os direitos autorais protegem as criações do espírito, ou seja, as obras intelectuais, intangíveis, que são facilmente digitalizadas e, consequentemente, disponibilizadas na internet. Justamente em razão do advento da rede mundial de computadores, facilitou-se a divulgação das obras intelectuais e sua reprodução perfeita, a baixíssimo custo.

A proteção jurídica das obras intelectuais dá-se por meio de um direito de propriedade que é outorgado ao autor da obra. Cuida-se de uma interessante evolução do direito de propriedade, conforme estudamos na Seção 3.1. Nesse sentido, é interessante saber que, quando o direito protege determinada obra sob a tutela do direito de autor, existe uma relação entre o titular do direito de autor e a obra intelectual, que independe de outros fatores, como o suporte físico em que se encontra a obra fixada. Assim, por exemplo, caso alguém adquira um livro, ele se torna proprietário do suporte físico e não da criação intelectual em si, que está protegida pelos direitos autorais. Ao comprarmos um filme em *blu-ray,* estamos adquirindo a propriedade do disco, ou seja, o suporte físico no qual o filme (obra artística) está gravado digitalmente.

O modelo dos "direitos autorais" pertence ao sistema jurídico do direito continental, no qual o direito brasileiro se insere. Por outro lado, o regime jurídico do copyright é o análogo dos direitos autorais nos países de origem anglo-saxã, como Estados Unidos e Inglaterra. Os direitos autorais e o copyright são institutos jurídicos distintos, todavia, em face dos tratados internacionais de proteção da propriedade intelectual, como a Convenção de Berna e o Tratado TRIPs, testemunhamos uma tendência de uniformização da proteção conferida às obras. Inclusive, o fato de uma obra ser protegida por direitos autorais em um país, não significa que não o seja em um país que siga o modelo do copyright.

Assimile

De maneira simplificada, podemos conceituar o Direito de Autor como sendo o ramo do Direito que regula as relações jurídicas advindas da criação e da utilização econômica de obras intelectuais estéticas e compreendidas nas artes e nas ciências (BITTAR, Carlos Alberto. **Direito de autor**. 3. ed. Rio de Janeiro: Forense Universitária, 2000. p. 3).

O direito de autor brasileiro, como dito, segue a tradição do direito continental, no sentido de ser um direito de caráter subjetivo, dirigido à proteção do autor e sua prerrogativa de explorar com exclusividade sua obra, retirando-lhe os proveitos

econômicos. Já o copyright é mais pragmático e voltado ao aspecto da proteção patrimonial da obra em si.

Sob uma perspectiva histórica, sabemos que o Direito de Propriedade Intelectual e os Direitos Autorais passaram a ser melhor estudados (e valorizados) a partir do surgimento das tecnologias de replicação de conteúdo. Antes da invenção da imprensa mecânica, não existiam grandes discussões sobre a matéria. A valorização do autor, trazida pelos movimentos intelectuais da era moderna, e a expansão dos meios de reprodução das obras colocaram a questão no centro dos debates internacionais (PINHEIRO, 2013, p. 145).

Neste contexto, o principal diploma legal que regula os direitos autorais no Brasil é a Lei nº 9.610 de 1998, conhecida como Lei de Direitos Autorais (LDA). Referida lei, em seu artigo 7º, enumera as obras protegidas por tal sistema jurídico, quais sejam: I – os textos de obras literárias, artísticas ou científicas; II – as conferências, alocuções, sermões e outras obras da mesma natureza; III – as obras dramáticas e dramático-musicais; IV – as obras coreográficas e pantomímicas, cuja execução cênica se fixe por escrito ou por outra qualquer forma; V – as composições musicais, tenham ou não letra; VI – as obras audiovisuais, sonorizadas ou não, inclusive as cinematográficas; VII – as obras fotográficas e as produzidas por qualquer processo análogo ao da fotografia; VIII – as obras de desenho, pintura, gravura, escultura, litografia e arte cinética; IX – as ilustrações, cartas geográficas e outras obras da mesma natureza; X – os projetos, esboços e obras plásticas concernentes à geografia, engenharia, topografia, arquitetura, paisagismo, cenografia e ciência; XI – as adaptações, traduções e outras transformações de obras originais, apresentadas como criação intelectual nova; XII – os programas de computador; XIII – as coletâneas ou compilações, antologias, enciclopédias, dicionários, bases de dados e outras obras, que, por sua seleção, organização ou disposição de seu conteúdo, constituam uma criação intelectual.

Analisando o conteúdo da referida lei, observamos a existência de dois conjuntos de prerrogativas que sustentam tal norma, bem como formam o alicerce básico do direito autoral brasileiro. Tais conjuntos relacionam-se aos vínculos morais e pecuniários do titular com sua obra. São eles os direitos morais e os direitos patrimoniais.

Cada um desses dois conjuntos de direitos cumpre funções próprias: os direitos morais se relacionam à defesa da personalidade do criador, consistindo em verdadeiros óbices a qualquer ação de terceiros com respeito à sua criação. Já os direitos patrimoniais se referem à utilização econômica da obra, representando os meios pelos quais o autor dela pode retirar proventos pecuniários (BITTAR, 2000, p. 46). Neste contexto, apenas o autor pessoa física pode ser titular dos direitos morais. Por outro lado, uma pessoa jurídica pode adquirir os direitos patrimoniais sobre uma obra, sendo assim sua legítima titular.

Sabemos que a internet eleva as possibilidades de replicação de conteúdo exponencialmente. No Brasil, temos que qualquer cópia feita com fins lucrativos e sem a autorização expressa do autor pode ser considerada uma infração ou violação a estes direitos, tanto morais como patrimoniais.

Tecnologias como o Napster, Freenet e Gnutella, entre outras, disponibilizaram uma grande quantidade de conteúdo de forma absolutamente gratuita. A mecânica utilizada pelas citadas ferramentas permite a busca e cópia de dados e informações armazenadas nos computadores dos usuários conectados a um determinado site em determinado momento. O problema não decorre do compartilhamento dos arquivos em si, mas sim no fato de que tais arquivos foram provavelmente compartilhados de forma gratuita, sem autorização dos legítimos titulares das obras e sem o devido pagamento de royalties.

Vocabulário

Royalty: é uma palavra de origem inglesa que se refere a uma importância cobrada pelo proprietário de uma patente de produto, processo de produção, marca, entre outros, ou pelo autor de uma obra, para permitir seu uso ou comercialização.

A grande circulação indiscriminada de conteúdos provoca questionamentos quanto à legalidade das próprias tecnologias que proporcionam tal circulação, justamente em razão da falta de autorização por parte daqueles que detêm a propriedade intelectual sobre tais conteúdos. Por isso, testemunhamos o crescimento das iniciativas de combate à pirataria e de outras práticas ilícitas na internet. Um exemplo disso, foi o projeto de lei norte-americano que visava combater atividades desde a distribuição, publicação ou transmissão não autorizada de conteúdos protegidos, passando pelo comércio de serviços e produtos "perigosos", chegando inclusive a extrapolar questões ligadas à própria territorialidade dos Estados Unidos. Foi o chamado SOPA (Stop On-line Piracy Act).

Reflita

Você considera que a culpa pela distribuição descontrolada de conteúdos protegidos por direitos autorais, sem a devida legalidade, é da tecnologia, como os provedores de serviço *peer-to-peer* (Napster, Torrent etc.), citados anteriormente? Ou seriam as pessoas os culpados? Atribuir responsabilidade aos provedores de aplicação é a maneira mais efetiva de parar a distribuição de conteúdo pirata?

O principal desafio de qualquer lei que visa proteger a propriedade intelectual refere-se justamente a garantir sua eficácia. Isso só ocorrerá quando todos os envolvidos, provedores de acesso, conexão, usuários, empresas etc. se engajarem num processo de proteção das obras imateriais, acabando com a cultura da pirataria, muito marcante, por exemplo, na cultura brasileira e de outros países.

Enquanto isso não ocorre, presenciamos uma espécie de "crise" no sistema de direitos autorais, decorrente tanto de fatores de ordem tecnológica como de fatores de ordem jurídica. Como vimos anteriormente, a evolução tecnológica gera uma crise nas instituições de Direito Autoral em decorrência da maior facilidade de fixação das obras em suportes materiais intangíveis (digitais).

Tendo em vista essas consequências, faz-se necessária uma releitura conceitual das instituições de Direito Autoral, no sentido de acompanhar a nova realidade tecnológica. Conceitos como criação, obra, fixação, reprodução, contrafação etc., não têm mais o mesmo conteúdo com que foram originalmente pensadas. Além disso, surgem novas noções como armazenamento digital em nuvem, codificação, compartilhamento por redes sociais, execução por streaming de vídeos, entre outras (POLI, 2008, p. 141).

Nesse sentido, é possível afirmar que a Lei de Direitos Autorais não será suficiente para regular as várias inovações tecnológicas. Igualmente, o Judiciário, de uma maneira geral, não está capacitado para decidir sobre questões que exigem o estudo constante, permeado por diversos aspectos técnicos.

Além disso, tem-se que algumas instituições, como o Escritório Central de Arrecadação e Distribuição (ECAD), responsável por centralizar a arrecadação e distribuição dos direitos autorais de execução pública musical, cumprindo seu papel protetivo em relação aos autores, estão sempre observando o aparecimento de modelos tecnológicos que colocam em risco o *status quo* do mercado.

Pesquise mais

Recentemente, ocorreu um intenso debate entre nossos legisladores acerca da legalidade do pagamento de direito autorais sobre as tecnologias *streaming*, como Netflix e Spotify. As posições divergentes foram muito bem tratadas no artigo **A legalidade do pagamento de direitos autorais relativos à execução pública sobre o *streaming***, de autoria da advogada Milena Grado. Disponível em: <http://pppadvogados.com.br/publicacoes/a-legalidade-do-pagamento-de-direitos-autorais-relativos-a-execucao-publica-sobre-o-streaming>. Acesso em: 23 ago. 2016.

Esse "engessamento" legislativo aliado à ineficácia do Poder Judiciário tem como consequência a criação de ferramentas advindas da própria iniciativa privada, com objetivo de flexibilizar e adequar os direitos autorais a esta nova realidade. Como vimos na Seção 1.1, trata-se da autorregulamentação típica do Direito Eletrônico.

Exemplificando

Exemplos de ferramenta originadas a partir da vontade do setor privado são: o projeto *Creative Commons* (https://br.creativecommons.org/) e os movimentos de Software Livre e *Open Source*.

Sem medo de errar

Suponha que, após finalizado, o software encomendado pela empresa é distribuído anonimamente na internet. A partir dessa distribuição é criada uma cópia pirata em que o nome de outra pessoa, e não o seu, aparece como criador daquele programa. Você, como autor, pode vindicar algum direito sobre aquela obra?

Atenção

O principal diploma legal que regula os direitos autorais no Brasil é a Lei nº 9.610 de 1998, conhecida como "Lei de Direitos Autorais " (LDA). Analisando o conteúdo da referida lei, observamos a existência de dois conjuntos de prerrogativas que sustentam tal norma, bem como formam o alicerce básico do direito autoral brasileiro. Tais conjuntos relacionam-se aos vínculos morais e pecuniários do titular com sua obra. São eles os direitos morais e os direitos patrimoniais.

Como vimos anteriormente, os Direitos Autorais são basicamente formados pelos direitos de cunho moral e patrimonial. Os direitos morais se relacionam à defesa da personalidade do criador, consistindo em verdadeiros óbices a qualquer ação de terceiros com respeito à sua criação. Já os direitos patrimoniais se referem à utilização econômica da obra, representando os meios pelos quais o autor dela pode retirar proventos pecuniários. Neste contexto, apenas o autor pessoa física pode ser titular dos direitos morais. Por outro lado, uma pessoa jurídica pode adquirir os direitos patrimoniais sobre uma obra, sendo assim sua legítima titular. Assim, caso seja criada uma cópia pirata do programa desenvolvido, no qual o nome de outra pessoa, e não o seu, aparece como criador daquele programa, seria possível que você, na condição de autor, vindicasse os direitos morais sobre a obra. Neste caso específico, o direito de paternidade sobre o programa, conceito este que será

melhor analisado na Seção 3.4. Quanto aos direitos patrimoniais, estes caberiam à empresa que encomendou o programa criado.

Avançando na prática

Direitos autorais, execução pública e tecnologias *streaming*

Descrição da situação-problema

Você, atuando na condição de desenvolvedor de programa de computador, criou uma plataforma on-line de *streaming* de vídeos. Referida plataforma tem por objetivo oferecer, de maneira gratuita para seus usuários, conteúdos de filmes e séries, protegidos por direitos autorais. Tais conteúdos somente são reproduzidos após comando específico do usuário, ou seja, são verdadeiros vídeos "por demanda". Você, como titular da plataforma, deverá pagar direitos autorais ao ECAD sobre tais conteúdos, em razão de eventual execução pública das obras?

Lembre-se

A execução pública tem fundamento no uso público. O significado de uso público é, na verdade, um uso pelo público, que, neste caso, é um conjunto de espectadores. A cobrança de direitos autorais sobre execução pública está hoje no Brasil sob a tutela do ECAD – Escritório Central de Arrecadação e Distribuição.

Resolução da situação-problema

A colocação à disposição do público é o ato de tornar mais acessível ao público e o ato de comunicação ao público é ato mediante o qual a obra é colocada ao alcance do público. Nesses dois conceitos, a diferenciação ocorre em função da palavra público, que na primeira significa um conjunto de pessoas, uma população e, no segundo, significa um conjunto de espectadores. Para que se configure um conjunto de espectadores é necessário o aspecto da simultaneidade. Dessa forma, a cobrança pelos direitos de autor sobre a execução pública no caso de *streaming* só é possível nos serviços de *live streaming*, que possuem a característica de contemporaneidade da recepção pelos espectadores. Os serviços de *streaming on demand* ("por demanda") configuram-se apenas como colocação à disposição do público e não há razão para a cobrança pelo ECAD, porque não é formada uma plateia ou uma audiência, não há simultaneidade, e cada uma das pessoas tem acesso individual, em um momento distinto. Logo, a cobrança pelo ECAD de direitos autorais sobre a execução pública deve recair somente pela modalidade *live streaming,* que permite a configuração de público na acepção do conceito de comunicação ao público e, consequentemente, de execução pública, uma vez que há simultaneidade na recepção da obra pelos espectadores.

Faça valer a pena

1. Sobre a relação do direito de autor com o Direito Eletrônico, assinale a alternativa incorreta:

a) Tal relação pode ser explicada tendo em vista que os direitos autorais protegem obras intelectuais, facilmente digitalizadas e, consequentemente, disponibilizadas na internet.

b) A divulgação das obras intelectuais e sua reprodução perfeita, a baixíssimo custo, foi facilitada pelo advento da internet.

c) A circulação de conteúdos digitais que infringem direitos autorais provoca questionamentos quanto à legalidade das próprias tecnologias que proporcionam tal circulação.

d) A evolução tecnológica gera uma crise nas instituições de Direito Autoral em decorrência da maior facilidade de fixação das obras em suportes materiais intangíveis (digitais).

e) O "engessamento" legislativo aliado à ineficácia do Poder Judiciário tem como consequência a criação de ferramentas advindas, em sua maioria, da iniciativa pública, com o objetivo de flexibilizar e adequar os direitos autorais a uma nova realidade.

2. Sobre os diferentes sistemas jurídicos de proteção das obras autorais, assinale a alternativa incorreta:

a) O modelo dos "direitos autorais" pertence ao sistema jurídico do direito continental, no qual o direito brasileiro se insere.

b) O regime jurídico do copyright é o análogo dos direitos autorais nos países de origem anglo-saxã, como Estados Unidos e Inglaterra.

c) Os direitos autorais e o copyright são institutos jurídicos distintos, todavia, em face dos tratados internacionais de proteção da propriedade intelectual, percebe-se uma tendência de uniformização da proteção conferida às obras.

d) O fato de uma obra estar protegida por direitos autorais em um país significa que não estará protegida em outro país que segue o modelo do copyright.

e) O direito de autor brasileiro é um direito de caráter subjetivo, dirigido à proteção do autor e sua prerrogativa de explorar com exclusividade sua obra, retirando-lhe os proveitos econômicos.

3. Acerca da evolução do Direito de Propriedade Intelectual, considere as seguintes assertivas:

I – Sob uma perspectiva histórica, sabe-se que o Direito de Propriedade Intelectual e os Direitos Autorais passaram a ser melhor estudados a partir do surgimento das tecnologias de replicação de conteúdo.

II – A valorização do autor trazida pelos movimentos intelectuais da era moderna e a expansão dos meios de reprodução das obras colocaram os direitos autorais no centro dos debates internacionais.

III – Grandes discussões envolvendo os Direitos Autorais eram frequentes, a nível internacional, mesmo antes da invenção da imprensa mecânica.

Estão corretas as assertivas:

a) I, apenas.

b) I e II.

c) I e III.

d) II e III.

e) II, apenas.

Seção 3.4

Proteção jurídica do software

Diálogo aberto

Na Seção 3.3, estudamos as questões ligadas ao direito de autor e às novas tecnologias. Nosso foco de estudo foi a Lei nº 9.610/1998, que confere as regras de proteção das obras salvaguardadas por direito de autor. Dentre tais obras, vimos também que estão incluídos os programas de computador. Pois bem, nesta seção, iremos aprofundar a análise relacionada à proteção jurídica dos programas de computador, ou software.

Para tanto, devemos antes retomar brevemente nossa situação geradora de aprendizagem (SGA): você foi contratado por uma empresa de engenharia para desenvolver um software do tipo CAD (desenho assistido por computador), destinado à criação de modelos tridimensionais de estruturas. A contratação foi realizada verbalmente, não tendo sido redigido nenhum contrato. Finalizado o projeto, a empresa registrou o software junto ao Instituto Nacional da Propriedade Intelectual (INPI). Tal software tornou-se conhecido pelos concorrentes da empresa de engenharia, que o contrataram para desenvolver solução idêntica. A empresa original que registrou o software entrou com uma ação na justiça contra você requerendo danos pela contrafação, ou venda não autorizada do software.

Considere a seguinte situação-problema: O contrato de desenvolvimento de software foi realizado de maneira verbal, não tendo sido nada acordado em relação à sua titularidade. Nestas condições, quem é o titular do software? Você, na condição de criador do software, tem algum direito sobre ele? O registro realizado pela empresa é legítimo? Uma vez desenvolvida solução idêntica para um concorrente, a ação judicial proposta tem fundamento?

Para resolvermos este problema, devemos aprofundar nossos estudos acerca da tutela jurídica do programa de computador, de modo a analisarmos a proteção conferida pela Lei de Direito Autoral, bem como pela Lei de Propriedade Industrial, analisando a questão da patentabilidade do software. Iremos traçar um panorama geral da Lei do Software, que define regras específicas para proteção e uso dos programas de computador. Iremos estudar também algumas outras questões, como registro, prazo de proteção e titularidade do software.

Não pode faltar

A cada dia, testemunhamos um aumento significativo da dependência de nossa sociedade por programas de computador. Tal fato é facilmente explicado, ao passo que o objetivo principal de um programa de computador é atender a uma necessidade ou resolver um problema específico, automatizando sistemas e processos. A popularização de dispositivos móveis, sobretudo do smartphone, provocou o aumento da criação dos chamados "aplicativos", que nada mais são do que programas de computador. Trata-se da verdadeira "corrida do ouro" moderna, sendo que frequentemente somos surpreendidos pelas cifras milionárias envolvendo a venda de empresas que criaram aplicativos revolucionários ou extremamente populares.

Dessa maneira, torna-se fundamental conhecermos a legislação que visa proteger e regular o uso de programas de computador. O software, ou programa de computador, é objeto de proteção de dois modelos complementares de proteção exclusiva, considerando o arcabouço de normas legais inseridas no Direito de Propriedade Intelectual (BARBOSA, 2010).

Assimile

De acordo com o artigo 1º da "Lei do Software", programa de computador é "a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados".

O primeiro modelo refere-se ao sistema da Lei nº 9.609/1998, que se volta ao programa de computador, em regime especial, e que se complementa pelas normas autorais gerais, reguladas pela Lei nº 9.610/1998, estudada na Seção 3.3. O segundo modelo diz respeito ao sistema de patentes de invenção, que protege soluções técnicas construídas através de programas de computador, soluções essas que se voltam aos problemas técnicos, ou seja, "inventos de software".

O foco do nosso estudo será nos modelos de proteção citados, ainda que o software, como tantos outros objetos de criação do espírito humano, seja também sujeito à tutela pela concorrência desleal, e pelo direito comum, como o direito civil. É possível ainda que o software não encontre proteção por qualquer sistema de direito ou que, ainda que protegido, circule sob algum tipo de norma privada de acesso livre, como as chamadas licenças *open source*. Analisaremos doravante

a proteção jurídica do software tanto em âmbito nacional quanto internacional, sobretudo pelas leis de direitos autorais.

Vocabulário

As **licenças *open source*** determinam que um programa de computador com "código aberto" deve garantir a distribuição livre desse programa. Tais licenças não devem restringir, de maneira nenhuma, a venda ou distribuição do programa, como componente de outro programa ou não. É importante diferenciar as licenças *open source* do movimento software livre. Basicamente, a diferença é que no *open source* o código-fonte do programa está aberto para consulta, e dependendo da vontade do criador, também para distribuição e redistribuição sob determinadas condições. O software livre implica em não propriedade do software. O *open source* pode ter um dono, por exemplo, os *drivers* da Nvidia, que são *open source*, com o código-fonte podendo ser acessado por terceiros, mas somente a própria Nvidia está autorizada a promover alterações. Um exemplo de software livre é o sistema Linux.

Reflita

Os movimentos *open source* e software livre trazem mais vantagens ou desvantagens para o mercado de desenvolvimento de programas de computador? O modelo de software proprietário cria mais incentivos, gerando mais riquezas?

Como dito anteriormente, o software é protegido essencialmente pelas normas contidas na Lei nº 9.609/1998 (Lei do Software), complementadas pela Lei nº 9.610/1998 (Lei de Direitos Autorais). A proteção também existe na Constituição Federal, em seu artigo 5º, inciso XXVII, no Código Civil, em seus artigos que regulam a responsabilidade civil, na Lei de Propriedade Industrial, quando trata de Patentes e Concorrência Desleal, bem como no Código Penal, em seu artigo 184.

O legislador pátrio optou em inserir o software no rol de obras protegidas pela Lei de Direitos Autorais, conforme se depreende do artigo 7º, inciso XII do citado diploma legal, além do artigo 2º da própria Lei do Software. Cumpre salientar que, enquanto conjunto de instruções, códigos ou estrutura, o programa de computador em si nunca será objeto de proteção por patente, por ser uma forma de expressão, assim como uma poesia ou uma música, e não uma solução técnica. Vale dizer que o programa de computador, naquilo que é objeto de direito autoral, é excluído da patentabilidade.

Quando a Lei do Software evoca a proteção dos programas de computador pelos direitos autorais e conexos, estes são inseridos no arcabouço das normas de Direito Internacional, entendendo-se como tal, às convenções e tratados internacionais. Todavia, cumpre destacar que nenhum tratado, convenção, pacto ou qualquer outro acordo celebrado entre países se sobrepõem às leis domésticas. O direito interno é sempre soberano.

O sistema internacional da Propriedade Intelectual se ampara em dois documentos básicos gerados no século XIX, dos quais o Brasil é signatário. Sem dúvida são os mais antigos e, provavelmente, os mais relevantes instrumentos multilaterais em relação à atividade econômica e à produção cultural, porém, essencialmente econômica.

O primeiro documento é chamado de Convenção da União de Paris para a Proteção da Propriedade Industrial, de 1883. A lista de participantes dessa convenção avulta conspicuamente duas classes: empresas e agentes de Propriedade Intelectual. Nas discussões estavam notoriamente ausentes os inventores e autores, já que o processo de negociação foi rigorosamente econômico e privado (BARBOSA, 2010).

O outro documento veio a se denominar Convenção de Berna de 1886. O alcance e objetivo dessa convenção é o das obras literárias e artísticas, incluindo aquelas de caráter científico. Assim, não só os livros ou esculturas, objetos tradicional de proteção, são abrangidos pela Convenção de Berna, mas também os programas de computador.

Obviamente, a proteção do software não foi prevista nas convenções do século XIX anteriormente citadas. A primeira previsão expressa, em escala multilateral, de sua proteção ocorre no TRIPs (Trade-Related Aspects of Intellectual Property Rights), de 1994, especificamente em seu artigo 10. O Acordo TRIPs tornou coativa a proteção do software por algum regime autoral. Por fim, a proteção do software é também objeto do Tratado de Direitos Autorais da Organização Mundial da Propriedade Intelectual (WIPO), do qual o Brasil não é signatário.

Como dito anteriormente, o programa de computador, quando considerado por si só (conjunto de instruções, código ou estrutura), é protegido pelas normas de direito autoral. Entretanto, isso não quer dizer que um software possa vir a ser objeto de uma patente. São as chamadas "invenções implementadas por softwares".

No que se refere a tais invenções, o Brasil está em consonância com o TRIPs em seu artigo 27 (1). Tal artigo determina que patentes devam ser concedidas para quaisquer produtos e processos, em qualquer área da tecnologia, desde que sejam novos, envolvam um passo inventivo e sejam passíveis de aplicação industrial.

Além de não haver qualquer impedimento legal, o Instituto Nacional da Propriedade Intelectual (INPI) também possui diretrizes para o exame de pedidos de patentes envolvendo invenções implementadas por programa de computador. Tais diretrizes compreendem definições, explicações e exemplos que ajudam, não só o examinador brasileiro em seu trabalho, mas qualquer inventor que almeje depositar um pedido de patente para proteger uma invenção implementada por software.

O INPI, por sua vez, entende que um pedido de patente relacionado a uma criação industrial passível de ser implementada por programa de computador é considerada patenteável se, a solução ali proposta e definida na forma de um método ou processo, apresenta um efeito técnico capaz de resolver um problema encontrado na técnica. Sendo que a solução não deve estar unicamente relacionada ao modo como o programa de computador é escrito, isto é, ao programa de computador em si (conjunto de instruções, código ou estrutura).

O INPI considera como "efeito técnico" os efeitos obtidos na realização das etapas definidas pelo método reivindicado na invenção implementada por programa de computador. Tal "efeito técnico" é basicamente medido pela contribuição da invenção frente ao estado da técnica. Ou seja, no exame do objeto reivindicado, tal método ou processo poderá ser considerado invenção desde que seus efeitos resultantes sejam técnicos e não simplesmente matemáticos.

Exemplificando

Alguns dos efeitos técnicos podem ser, por exemplo, melhoria (não apenas estética) da interface com o usuário, otimização dos tempos de execução de um processo, aperfeiçoamento de recursos, como uso da memória, gerenciamento e transmissão de dados e arquivos.

Por outro lado, alterações no código-fonte do programa que tragam o benefício de maior velocidade, menor tamanho (seja do código-fonte ou do espaço ocupado em memória), modularidade etc., apesar de serem efeitos técnicos, pertencem ao âmbito do programa de computador em si, portanto, excluídos da patentabilidade.

Não existe qualquer restrição legal fora dos padrões mundiais às patentes de software no Brasil ou qualquer preconceito por parte do INPI para sua proteção. Não é fundamental que o programa de computador esteja necessariamente acoplado a um hardware para ser patenteável. Na verdade, o que é realmente importante é que o pedido de patente de invenção implementada por software esteja corretamente elaborado de modo a compreender uma solução proposta e definida na forma de um método ou processo novo que apresente um efeito técnico que resolva um problema existente.

Definida a questão da "patente de software", que na verdade se trata da patentabilidade de invenções implementadas por softwares, iremos agora analisar a proteção jurídica conferida ao "software em si", a qual é conferida, fundamentalmente, pelas Leis nº 9.609/1998 e 9.610/1998. Não é nossa intenção analisar a Lei do Software artigo por artigo, mas prover um panorama geral, de modo a estabelecer os conhecimentos necessários para proteção da obra.

Inicialmente, a proteção dupla do programa de computador, tanto pela Lei do Software quanto pela Lei de Direitos Autorais, é resultado da intenção do legislador, que no artigo 2º daquela prevê expressamente que a proteção à propriedade intelectual de programa de computador é a conferida às obras literárias pela legislação de direitos autorais. Assim, a aplicação da Lei de Direitos Autorais é subsidiária, ou seja, sua validade é limitada pelas disposições da Lei do Software.

Quanto aos direitos conferidos, você se lembra da divisão existente na Lei de Direitos Autorais, estudada na Seção 3.3, entre direitos morais e patrimoniais dos autores? Pois bem, essa divisão está presente também na Lei do Software. Todavia, no tocante aos direitos morais, essa aplicação é muito mais restrita, sendo que somente são reconhecidos ao autor de programa de computador o direito à autoria (paternidade) e o direito à integridade do programa. Nesta última, o autor só poderá se opor a modificações que prejudiquem a obra ou atinjam sua reputação. Quanto aos direitos patrimoniais, estes são idênticos, sendo vedado qualquer uso não autorizado do programa de computador. Porém, existe uma exceção, que é a chamada cópia de segurança ou salvaguarda, a qual o usuário poderá manter sem que isso configure a contrafação.

A proteção do programa de computador possui um limite temporal de 50 anos, contados a partir de 1º de janeiro do ano seguinte à publicação da obra. Assim, como as obras literárias, a proteção do software independe de registro. Todavia, o registro do programa, o qual é realizado perante o INPI, traz alguns benefícios, como presunção de autoria e segurança jurídica, podendo, inclusive, ser feito em nome de pessoa jurídica. Porém, deverá ser sempre indicada uma pessoa física como autora da obra.

Pesquise mais

Para conhecer melhor o procedimento de registro de um programa de computador, acesse o site oficial do INPI. Disponível em: <http://www.inpi.gov.br/menu-servicos/programa-de-computador>. Acesso em: 23 ago. 2016.

A titularidade do programa é, em regra, do próprio criador. Mas a Lei do Software, em seu artigo 4º, prevê que, quando o programa for elaborado sob um vínculo trabalhista ou estatutário, os direitos a ele relativos pertencerão exclusivamente ao empregador ou órgão público. O mesmo vale para as hipóteses de contratação de serviços específicos. Ou seja, quando uma empresa contrata outra para desenvolver um software, os direitos relativos a este pertencerão à empresa contratante, salvo disposição em contrário. Por isso, é importante sempre constar num contrato de desenvolvimento ou licenciamento de programa de computador a quem pertencerão os direitos de propriedade intelectual sobre a obra finalizada.

Por fim, a proteção à obra e seu criador se dá tanto na esfera cível quanto na esfera penal, sendo que eventuais violações podem ser punidas, por exemplo, com o pagamento de indenização pecuniária ou, ainda, com a prisão do infrator.

Sem medo de errar

Vistos os principais conceitos, vamos resolver nossa situação-problema: o contrato de desenvolvimento de software foi realizado de maneira verbal, não tendo sido nada acordado em relação à titularidade do software. Nestas condições, quem é o titular do software? Você, na condição de criador do software, tem algum direito sobre ele? O registro realizado pela empresa é legítimo? Uma vez desenvolvida solução idêntica para um concorrente, a ação judicial proposta tem fundamento?

Atenção

A titularidade do programa é, em regra, do próprio criador. Mas a Lei do Software, em seu artigo 4º, prevê que, quando o programa for elaborado sob um vínculo trabalhista ou estatutário, os direitos a ele relativos pertencerão exclusivamente ao empregador ou órgão público. O mesmo vale para as hipóteses de contratação de serviços específicos.

Tendo em vista que foi realizado um contrato verbal entre as partes e que, neste contrato, nada consta acerca da titularidade do software desenvolvido, é necessário recorrermos à regra geral contida no artigo 4º da Lei do Software (1998), que dispõe que:

> salvo estipulação em contrário, pertencerão exclusivamente ao empregador, contratante de serviços ou órgão público, os direitos relativos ao programa de computador, desenvolvido e elaborado durante a vigência de contrato ou de vínculo estatutário, expressamente destinado à pesquisa e desenvolvimento, ou em que a atividade do empregado, contratado de serviço ou servidor, seja prevista, ou ainda, que decorra da própria natureza dos encargos concernentes a esses vínculos.

Dessa maneira, a titularidade do software é da empresa que o contratou para desenvolvê-lo. Igualmente, o registro realizado pela empresa é legítimo, uma vez que é a titular da obra. Todavia, cumpre ressaltar que ao registrar o programa no INPI, deve a empresa indicar o "criador do programa", neste caso, você, sob pena de violação do direito de paternidade sobre o programa. Por fim, caso você crie uma solução idêntica e venda para os concorrentes, pode a empresa titular ingressar com medida judicial requerendo a respectiva indenização pelo uso não autorizado.

A título de curiosidade, caso a nova solução criada seja semelhante ao programa original, em razão das "características funcionais de sua aplicação, da observância de preceitos normativos e técnicos, ou de limitação de forma alternativa para a sua expressão", esta não poderá ser considerada como cópia, não constituindo ofensa aos direitos da empresa titular do software. Isto ocorre por força da norma contida no artigo 6º da Lei nº 9.609/1998.

Avançando na prática

Posso patentear um software?

Descrição da situação-problema

Você, na condição de desenvolvedor de software, foi contratado por uma empresa para otimizar um processo de compactação de arquivos feito por um programa de computador de titularidade da empresa. Por meio de uma alteração no código-fonte, você conseguiu reduzir significantemente o tempo do processo de compactação, bem como o tamanho final dos arquivos compactados. A solução criada foi muito bem quista na empresa, tendo em vista que a economia indireta gerada pela redução de custos agradou, inclusive, aos outros diretores. Diante desse cenário, o diretor de TI da empresa perguntou se teria jeito de "pedir a patente" da nova solução. Diante desta situação, o que você responderia ao diretor de TI?

Lembre-se

O INPI entende que um pedido de patente relacionado a uma criação industrial, passível de ser implementada por programa de computador, é considerada patenteável se, a solução ali proposta e definida na forma de um método ou processo, apresenta um efeito técnico capaz de resolver um problema encontrado na técnica. Sendo que a solução não deve estar unicamente relacionada ao modo como este programa de computador é escrito, isto é, ao programa de computador em si (conjunto de instruções, código ou estrutura).

Resolução da situação-problema

Primeiramente, é preciso esclarecer a questão relacionada à proteção do programa de computador pelas normas de direito de propriedade intelectual. O programa de computador é protegido por dois modelos diferentes. O primeiro modelo refere-se ao sistema da Lei nº 9.609/1998, que se volta ao programa de computador, em regime especial, e que se complementa pelas normas autorais gerais, reguladas pela Lei nº 9.610/1998. O segundo modelo diz respeito ao sistema de patentes de invenção, que protege soluções técnicas construídas através de programas de computador, soluções essas que se voltam aos problemas técnicos, ou seja, "inventos de software".

O INPI entende que um pedido de patente relacionado a uma criação industrial passível de ser implementada por programa de computador é considerada patenteável se, a solução ali proposta e definida na forma de um método ou processo, apresenta um efeito técnico capaz de resolver um problema encontrado na técnica. Sendo que a solução não deve estar unicamente relacionada ao modo como este programa de computador é escrito, isto é, ao programa de computador em si (conjunto de instruções, código ou estrutura).

Dessa maneira, uma solução como aquela proposta no problema, advinda exclusivamente de uma alteração no código-fonte do software, não é patenteável. Todavia, é possível realizar um aditamento no registro do software perante o INPI, ou mesmo, realizar um novo registro, caso a alteração implique no advento de uma nova obra derivada, diferente da original. O importante é que fique claro que tal modificação estará protegida pelas normas específicas e de direito de autor (Leis nºs 9.609/1998 e 9.610/1998).

Faça você mesmo

No ano de 2015, o INPI divulgou uma série de diretrizes discutindo critérios para concessão de patentes, inclusive de software. Caso queira saber mais sobre este intrincado procedimento, sugerimos a leitura do artigo intitulado **INPI discute critérios de patentes, inclusive para software**, de Luís Osvaldo Grossmann. Disponível em: <http://m.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=39169&sid=33>, bem como do documento indicado ao final desta reportagem no endereço ,http://convergenciadigital.uol.com.br/inf/patenteabilidade032015.pdf>. Acesso em: 23 ago. 2016.

Faça valer a pena

1. Considere as seguintes afirmativas:

I – O software é objeto de proteção de dois modelos complementares de proteção exclusiva, considerando o arcabouço de normas legais inseridas no Direito de Propriedade Intelectual.

II – Um dos modelos de proteção do software refere-se ao sistema da Lei nº 9.609/1998, que se volta ao programa de computador, em regime especial, e que se complementa pelas normas autorais gerais, reguladas pela Lei nº 9.610/1998.

III – Um dos modelos de proteção do software diz respeito ao sistema de desenho industrial, que protege soluções técnicas construídas através de programas de computador, soluções essas que se voltam aos problemas técnicos, ou seja, "inventos de software".

Estão corretas as afirmativas:

a) I, apenas.

b) I e II.

c) II e III.

d) I e III.

e) I, II e III.

2. Assinale a alternativa que apresenta a principal diferença entre softwares "*open source*" e "softwares livres":

a) Os software *open source* possuem código aberto para consulta, enquanto os softwares livres não possuem.

b) Os softwares livres possuem código aberto para consulta, enquanto os software *open source* não possuem.

c) O software livre implica em não propriedade do software, já o software *open source* pode ter um dono.

d) Os software livres possuem o código-fonte aberto para consulta, e dependendo da vontade do criador, também para distribuição e redistribuição sob determinadas condições.

e) O software *open source* implica em não propriedade do software, já o software livre pode ter um dono.

3. A primeira previsão expressa, em escala internacional multilateral, de proteção do software foi feita em qual dos Tratados abaixo?

a) Convenção de Berna.

b) Lei nº 9.610/1998.

c) Tratado de Direitos Autorais da Organização Mundial da Propriedade Intelectual.

d) Acordo TRIPs.

e) Lei nº 9.609/1998.

Referências

BARBOSA, Denis Borges. **Tratado da propriedade intelectual**. Rio de Janeiro: Lumen Juris, 2010. t. 3.

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

BRASIL. Lei nº 9.279, de 14 de maio de 1996. maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. **Diário Oficial da União**, Brasília, DF, 15 maio 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9279.htm>. Acesso em: 15 ago. 2016.

_____. Lei nº 9.610, de 19 de fevereiro de 1998. fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. **Diário Oficial da União**, Brasília, DF, 20 fev. 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9610.htm>. Acesso em: 15 ago. 2016.

_____. Lei nº 9.609 , de 19 de fevereiro de 1998. fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 20 fev. 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9609.htm>. Acesso em: 15 ago. 2016.

FARAH, R. M. **IP NAT**: a responsabilidade dos provedores de conexão. Disponível em:<http://pppadvogados.com.br/publicacoes/ppp-news-autorconvidado-3>. Acesso em: 23 ago. 2016.

GRADO, Milena. **A legalidade do pagamento de direitos autorais relativos à execução pública sobre o *streaming***. Disponível em: <http://pppadvogados.com.br/publicacoes/a-legalidade-do-pagamento-dedireitos-autorais-relativos-a-execucao-publica-sobre-o-streaming>. Acesso em: 23 ago. 2016.

GROSSMANN, L. O. **INPI**. Disponível em: <http://m.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=39169&sid=3>. Acesso em: 23 ago. 2016.

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

POLI, Leonardo Macedo. **Direito autoral**: parte geral. Belo Horizonte: Del Rey, 2008.

ROHRMANN, Carlos Alberto. **Curso de direito virtual**. Belo Horizonte: Del Rey, 2005.

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

Crimes eletrônicos

Convite ao estudo

Chegamos finalmente à última unidade do nosso curso. Ao longo deste tempo, estudamos diversos aspectos do Direito Eletrônico, desde os fundamentos técnicos da internet, passando pelas características desse ramo do Direito, até questões jurídicas mais específicas, como a responsabilidade dos provedores e os problemas ligados à propriedade intelectual. Nesta unidade iremos estudar um assunto que desperta muito interesse das pessoas ligadas à área técnica de tecnologia da informação. Trata-se do estudo dos crimes eletrônicos, ou informáticos.

Em que pese a popularização da figura do *hacker* remontar desde a década de 1980, somente recentemente o Brasil entrou para o grupo de países que possuem legislação específica sobre o tema. Nosso objetivo, nesta unidade, é justamente estudar as normas penais que visam coibir a prática de delitos informáticos, como a Lei nº 12.737/2012, a chamada Lei Carolina Dieckmann.

Para tanto, iremos considerar a seguinte Situação Geradora de Aprendizagem (SGA): Você foi contratado por uma empresa na área de tecnologia da informação para o cargo de analista de segurança da informação. Uma de suas atribuições é analisar e medir o nível de capacitação dos funcionários e colaboradores acerca dos riscos de segurança da informação, como vazamento de dados, disseminação de códigos maliciosos, entre outros. Para tanto, você teve a ideia de realizar um "teste de penetração" (pentest), simulando o ataque de uma fonte maliciosa. Todavia, para tornar o teste o mais realista possível, você avisou somente seu superior hierárquico. Uma vez executado o teste, o mesmo gerou o caos entre diversos setores, que ficaram contrariados com o pânico momentâneo causado. Diante deste cenário responda: a conduta descrita (pentest) pode ser classificada como um crime informático? Seria ele próprio ou impróprio? A conduta descrita pode ser enquadrada no tipo penal "Invasão a dispositivo informático"?

Estas e outras questões serão esclarecidas ao longo desta unidade. Na Seção 4.1, iremos abordar alguns conceitos básicos do Direito Penal, contextualizando-os à nossa matéria. Na Seção 4.2, estudaremos as

condutas que podem ser classificadas como crimes informáticos próprios ou impróprios, analisando detidamente cada uma delas. Na Seção 4.3, iremos aprofundar nossos estudos na Lei nº 12.737/2012, a chamada Lei Carolina Dieckmann, trazendo todos os aspectos técnicos e controvérsias dos tipos penais lá previstos. Por fim, na Seção 4.4, estudaremos algumas questões controvertidas, como tempo do crime, lugar do crime, concurso de pessoas, entre outras.

Seção 4.1

Breve introdução ao direito penal

Diálogo aberto

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 por parte de empresas e profissionais de TI.

Neste sentido, vamos retomar nossa SGA: uma vez executado o pentest, ele gerou o caos entre diversos setores, que ficaram contrariados com o pânico momentâneo causado. A partir desta SGA, considere a seguinte situação-problema: Caso alguém que não sabia que a situação se tratava de um teste, registrar um boletim de ocorrência junto a uma Delegacia Especializada, é possível classificar a conduta como um delito informático? Como realizar tal análise?

Para responder a este questionamento, iremos estudar, nesta Seção 4.1, alguns conceitos básicos do direito penal brasileiro, como o princípio da legalidade, também conhecido como princípio da reserva legal. Vamos estudar a teoria da tipicidade e o fato típico, trazendo a classificação dos crimes informáticos entre próprios e impróprios, além de alguns conceitos e terminologias utilizados pelos operadores do direito para se referir aos sujeitos ativos e passivos desse tipo de crime, como *hackers, crackers, phreakers*, bem como as ferramentas mais utilizadas por criminosos.

Não pode faltar

Conforme vimos ao longo deste curso, os computadores, atualmente, estão presentes em nosso cotidiano, inclusive criando situações de dependência, como o controle de tráfego aéreo ou a contabilização das atividades realizadas por um caixa bancário. Igualmente, o benefício da internet é incomensurável, possibilitando desde uma simples pesquisa até o controle de infraestruturas complexas remotamente.

Na nossa primeira unidade, estudamos algumas características da rede mundial de computadores, dentre elas: a instantaneidade das comunicações, a eliminação de barreiras temporais e geográficas, e a possibilidade de autorregulamentação em relação às regras de condutas entre os usuários e provedores. Tais características trazem uma série de vantagens e liberdades. Entretanto, trazem também um lado mais sombrio, que se refere justamente ao uso da rede como ferramenta para prática dos mais diversos crimes.

A título de condutas antiéticas e criminosas, podemos citar sites de pornografia infantil, racismo, ofensa à honra das pessoas, desenvolvimento e disseminação de códigos maliciosos, tráfico de entorpecentes e outras drogas ilícitas, fraudes bancárias e até mesmo o ciberterrorismo.

Nesse sentido, a presença da internet no cotidiano das pessoas se tornou uma constante, não existindo mais possibilidade de volta ao passado, de forma que deve ser aceita e compreendida da melhor maneira possível, exigindo-se, para tanto, o estudo e a pesquisa dos fenômenos que lhes são afetos, tais como os crimes virtuais.

A figura do Estado, como ente interventor nas relações humanas, surge como substituto da autotutela punitiva ("olho por olho, dente por dente") e, para tanto, faz o uso de normas que estabelecem consequências para os que as transgredirem, a fim de se manter a ordem legal estabelecida. Tem-se aí o direito de punir, que está atrelado a alguns princípios e questões básicas, que merecem nossa análise de estudarmos os crimes informáticos propriamente ditos (FURLANETO NETO; SANTOS; GIMENES, 2012,. p. 17).

O primeiro princípio a ser estudado é o da legalidade ou, para alguns doutrinadores, da reserva legal. Especifica o artigo 5º, inciso XXXIX da Constituição Federal de 1988 que "não haverá crime sem lei anterior que o defina, nem pena sem prévia cominação legal". Por sua vez, o Código Penal Brasileiro, em seu artigo 1º estabelece que "não há crime sem lei anterior que o defina; não há pena sem prévia cominação legal". Tal princípio trata-se de verdadeira limitação ao poder do Estado de interferir nas liberdades dos indivíduos. Nesse contexto, nenhum fato pode ser considerado crime e nenhuma pena criminal pode ser aplicada, sem que antes desse mesmo fato exista uma lei prevendo tal conduta como crime, estabelecendo ainda a respectiva pena para esta.

Assimile

De acordo com o princípio da legalidade, nenhum fato pode ser considerado crime e nenhuma pena criminal pode ser aplicada, sem que antes desse mesmo fato exista uma lei prevendo tal conduta como crime, estabelecendo ainda a respectiva pena para esta.

A concepção atual do princípio da legalidade é obtida no quadro da denominada função de garantia da lei penal que provoca desdobramento do princípio em exame em quatro outros princípios (TOLEDO, 1991). Estes outros princípios são: a) *lex praevia*, que se refere à irretroatividade de leis que prevejam novos crimes ou agravem a pena daqueles já existentes; b) *lex scripta*, que não permite o uso do direito baseado em costumes para incriminar determinada ação ou para penalizar mais severamente os tipos já previstos; c) *lex stricta*, que proíbe o uso da analogia para esta mesma última finalidade e; d) *lex certa*, de acordo com o qual não podem existir leis penais indeterminadas (TOLEDO, 1991).

Com a utilização conjunta de tais princípios, na forma de uma modalidade maior que a todos englobe, perfaz-se o princípio da legalidade, de modo a que se dê a atuação da lei penal, individualmente, dentro de um sistema de garantias. Do princípio da legalidade, deriva-se a teoria da tipicidade que, por sua vez, veio a dar mais técnica ao aludido princípio.

"A tipicidade, num conceito preliminar, é a correspondência entre o fato praticado pelo agente e a descrição de cada espécie da infração contida na lei penal incriminadora" (JESUS, 1993, p. 230). Esta tipicidade dá o caráter punível e ressalta a importância criminal da conduta, amoldando-se ao modelo legalmente previsto, a fim de configurar-se o ilícito penal. Ela ocorre quando a ação apresenta as características objetivas e subjetivas do modelo legalmente formulado pelo legislador. Trata-se de verdadeira correspondência entre uma conduta da vida real e o tipo legalmente previsto na legislação penal.

De tal forma, percebe-se que o tipo "é o modelo legal do comportamento proibido, compreendendo o conjunto de características objetivas e subjetivas do fato punível. Tipo não é o fato delituoso em si, mas a descrição legal de um fato que a lei proíba ou ordena.

Em conclusão, podemos afirmar que a tipicidade e o fato típico, em conjunto com o princípio da legalidade ou reserva legal, têm a função político-criminal de evitar a prática de crimes previstos legalmente. Assim, as novas formas de violação de bens jurídicos (ex.: honra, vida, privacidade) através da internet, por se apresentarem como fato socialmente relevante e cada vez mais significativo, representam novo desafio a ser enfrentado pelo direito penal.

O surgimento dos crimes informáticos remonta à década de 1960, quando houve os primeiros registros do "uso do computador para a prática de delitos, constituídos, sobretudo, por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados em matérias jornalísticas" (FERREIRA apud LUCCA; SIMÃO FILHO, 2000, p. 209). Por sua vez, somente nos anos 1970 verificaram-se os estudos sistemáticos e científicos sobre essa matéria, com emprego de métodos criminológicos, relativos a delitos informáticos verificados

na Europa em instituições de renome internacional.

A criminalidade informática conta com as mesmas características do processo de informatização global: a) transnacionalidade: todos os países fazem uso da informatização, logo a correspondente delinquência está presente em todos os continentes; b) universalidade: integrantes de várias camadas sociais e econômicas já têm acesso aos produtos informatizados; c) ubiquidade: a informatização está presente em todos os setores e todos os lugares (GOMES, 2000).

Importante ressaltar que a doutrina não chegou a um consenso quanto a uma única nomenclatura, abordando a temática sobre o título de crimes virtuais, crimes digitais, crimes informáticos, crimes eletrônicos etc. Todavia, a boa técnica manda que se dê nome aos delitos com base no bem jurídico por ele protegido (VIANNA, 2003). Dessa maneira, a denominação "crimes virtuais" seria absurda, pois, ainda que se conceba que os crimes são praticados num mundo "virtual", não haveria qualquer sentido em se falar de um bem jurídico virtual. A denominação mais precisa, neste caso, seria "crimes informáticos", por basear-se no bem jurídico penalmente tutelado, que normalmente é a inviolabilidade das informações automatizadas. Porém, como dito anteriormente, a nomenclatura não é unânime.

Em rigor, para que um delito seja considerado informático, é necessário que o bem jurídico por ele protegido seja a inviolabilidade das informações. A simples utilização, por parte do agente, de um computador para a execução de um delito, por si só, não configuraria um crime informático, caso o bem jurídico afetado não fosse a informação automatizada. Ocorre, no entanto, que muitos autores acabaram, por analogia, denominando crimes informáticos os delitos em que o computador serviu como instrumento da conduta.

Nesse sentido, aos delitos em que o computador foi instrumento para a execução do crime, mas não houve ofensa ao bem jurídico "inviolabilidade de informações automatizadas", denominamos Delitos Informáticos Impróprios. Em contrapartida, aqueles em que o bem jurídico afetado foi a "inviolabilidade de informações automatizadas", denominamos delitos informáticos próprios. Aos delitos complexos em que, além da proteção da inviolabilidade de informações, a norma visa à tutela de bem jurídico diverso, denominamos Delitos Informáticos Mistos (VIANNA, 2003). Na próxima seção estudaremos detidamente cada uma das categorias acima mencionadas, analisando ainda as espécies de condutas que se encaixam em cada uma respectivamente.

Quantos aos sujeitos envolvidos no crime informático, temos os sujeitos ativos e os sujeitos passivos. Quando se menciona "criminoso", estamos nos referindo ao sujeito ativo do crime. Assim, em tese, qualquer pessoa pode ser um agente de crime de informática. Em geral, os criminosos virtuais diferem-se dos demais, pois possuem grande conhecimento técnico de sua área e não empregam instrumentos

e armas tradicionais, nem contato direto pessoal com a vítima. Diversas são as denominações utilizadas para indicar um criminoso virtual.

Temos os *hackers*, que são especialistas em informática, capazes de invadir dispositivos computacionais alheios, mas também, de impedir invasões de outros. Por sua vez, os *crackers*, atuam de forma claramente dolosa, isto é, com intenção de prejudicar alguém ou de tirar proveito para si ou para terceiros, a partir de um dado ou informação obtida. Existem ainda os *insiders*, que são os *hackers* internos de uma empresa, normalmente ocupando a condição de empregado ou colaborador. Igualmente, temos os *phreakers*, que utilizam de meios de comunicação mediante o emprego de artifícios fraudulentos, sem ter nenhum custo pelo serviço. Por fim, para complementar sua formação, temos o termo *lammer*, utilizado para as pessoas que possuem nenhum ou pouco conhecimento sobre hacking e utilizam ferramentas desenvolvidas por outros para realizarem seus ataques.

Do outro lado, temos os sujeitos passivos, ou seja, as vítimas. Qualquer pessoa poderá ser sujeito passivo deste tipo de crime. No geral, bastaria ter um computador para estar suscetível a estes delitos realizados com suporte da tecnologia da informação, mas não necessariamente, uma vez que pode ser vitimado por meio de pen drives ou CDs contaminados; pelo recebimento de um e-mail com códigos maliciosos, ter informações hospedadas em servidores utilizadas de maneira indevida etc.

Exemplificando

Um exemplo de dispositivo muito popular entre hackers, *insiders*, ou até especialistas em segurança da informação é o "*rubber ducky*". Trata-se de dispositivo que à primeira vista parece um pen drive comum, mas, na verdade, contém um teclado programado que ao ser conectado começa a escrever de forma automatizada, podendo executar programas, seja do próprio computador ou da memória Micro SD integrada. Este equipamento é muito perigoso, porque digitando os comandos apropriados, em segundos, pode-se acessar todo tipo de informação, e até mesmo enviá-la automaticamente para a internet.

Quanto a investigações formais destes crimes, tem-se 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. Isto porque, a internet, por ser um ambiente virtual de dimensões incalculáveis, proporciona várias formas de cometimentos deste tipo de crimes. Dentre estes 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 controle 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.

Uma observação é válida aqui no que diz respeito aos botnets ou redes zumbis, isto é, malhas de computadores infectados por malwares, controlados remotamente por cibercriminosos, e que são utilizados para coletar informações de cartões de crédito e dados de acesso de e-mail, de espionagem industrial; ataques de negações de serviços para extorquir empresas; spam e phishing; tornar computadores de uma rede em agentes de envio de e-mail para spammers; ou ainda para produzir cliques falsos, gerando receita ao anunciante.

E você já entrou em contato com alguma notícia ou ação envolvendo as botnets?

Por fim, vamos ressalvar que o combate à criminalidade informática encontra vários entraves relacionados às lacunas legislativas, mas não somente; também aos reflexos que podem causar restrição à liberdade de expressão e ao acelerado desenvolvimento tecnológico. No Brasil, as leis específicas são obsoletas, acarretando na atipicidade de vários atos. Outros problemas mais controversos também causam a sensação de impunidade frente a tais crimes, os quais estudaremos mais detidamente na Seção 4.4.

Reflita

A criação de normas penais específicas traria uma solução para a crescente onda de crimes informáticos? Na sua opinião, uma repressão muito forte por parte do Estado inibiria a liberdade de expressão e a democracia? O monitoramento da internet por parte de agências de inteligência como a NSA é necessário para evitar ataques cibernéticos de larga escala (ciberterrorismo)?

Pesquise mais

Para aprofundar seus conhecimentos sobre a questão da tipificação dos crimes informáticos, recomendamos a leitura do seguinte artigo disponível em: <http://www.egov.ufsc.br:8080/portal/conteudo/crimes-virtuais-elementos-para-uma-reflex%C3%A3o-sobre-o-problema-na-tipifica%C3%A7%C3%A3o>. Acesso em: 4 out. 2016.

Sem medo de errar

Vamos retomar nossa situação-problema: caso alguém que não sabia que a situação se tratava de um teste, registrar um boletim de ocorrência junto a uma delegacia especializada, é possível classificar a conduta como um delito informático? Como realizar tal análise?

Atenção

De acordo com o princípio da legalidade, nenhum fato pode ser considerado crime e nenhuma pena criminal pode ser aplicada, sem que antes desse mesmo fato exista uma lei prevendo tal conduta como crime, estabelecendo ainda a respectiva pena para esta.

Em rigor, para que um delito seja considerado informático, é necessário que o bem jurídico por ele protegido seja a inviolabilidade de informações. A simples utilização, por parte do agente, de um computador para a execução de um delito, por si só, não configuraria um crime informático, caso o bem jurídico afetado não fosse a informação automatizada. Ocorre, no entanto, que muitos autores acabaram, por analogia, denominando crimes informáticos os delitos em que o computador serviu como instrumento da conduta. Nesse sentido, aos delitos em que o computador foi instrumento para a execução do crime, mas não houve ofensa ao bem jurídico "inviolabilidade de informações automatizadas", denominamos delitos informáticos impróprios. Em contrapartida, aqueles em que o bem jurídico afetado foi a "inviolabilidade de informações automatizadas", denominamos delitos informáticos próprios. Aos delitos complexos em que, além da proteção da inviolabilidade de informações, a norma visar a tutela de bem jurídico diverso, denominamos delitos informáticos mistos. Ainda, para que uma conduta seja considerada criminosa, é necessária uma lei prévia prevendo tal conduta como crime, estabelecendo ainda a respectiva pena para esta.

Dessa maneira, a realização de um teste de penetração que venha a ocasionar danos a terceiro, pode ser classificado como delito informático, podendo ainda ser

próprio ou impróprio, a depender do bem jurídico atingido. Ainda, é necessário que a conduta esteja expressamente prevista em Lei, por força do princípio da legalidade.

Avançando na prática

Investigação forense computacional

Descrição da situação-problema

Ainda na condição de analista de segurança de informação de uma empresa, você foi nomeado pela diretoria para ajudar o Delegado titular da Vara Especializada em Crimes Informáticos de seu município em uma investigação a um ataque ocorrido aos servidores. Em uma investigação preliminar, verificou-se a presença de backdoors nos servidores da empresa. Diante dessa situação, o delegado pediu que você enviasse um relatório identificando o sujeito ativo e passivo do suposto crime, bem como o meio ou ferramenta provavelmente utilizado por ele.

Lembre-se

Quanto aos sujeitos envolvidos no crime informático, temos os sujeitos ativos e os sujeitos passivos.

Resolução da situação-problema

Ao elaborar o relatório, você deverá indicar os sujeitos envolvidos num crime informático, quais sejam, sujeitos ativos e os sujeitos passivos. Quando se menciona "criminoso", estamos nos referindo ao sujeito ativo do crime. Assim, em tese, qualquer pessoa pode ser um agente de crime de informática, cabendo à investigação policial chegar a uma conclusão quanto a este tópico. Do outro lado, temos os sujeitos passivos, ou seja, as vítimas. Qualquer pessoa poderá ser sujeito passivo deste tipo de crime. Neste caso, a vítima é a empresa, que teve seus sistemas de informações violados por terceiro. Quanto à ferramenta provavelmente utilizada pelo criminoso, tem-se que o criminoso possivelmente utilizou um Trojan, ou "Cavalo de Troia", que consiste em programa enviado 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.

Faça você mesmo

Para saber mais sobre os principais malwares utilizados por cibercriminosos, recomendamos a leitura desta cartilha elaborada pelo CGI. Disponível em: <http://cartilha.cert.br/malware/>. Acesso em: 4 out. 2016.

Faça valer a pena

1. Dentre as alternativas abaixo, assinale aquela que NÃO apresenta um exemplo de conduta antijurídica praticada pela internet:

a) Criação de sites de pornografia infantil.

b) Criação de sites falsos para prática de fraudes bancárias.

c) Criação de sites para venda de produtos diversos.

d) Disseminação de códigos maliciosos.

e) Ciberterrorismo.

2. "Nenhum fato pode ser considerado crime e nenhuma pena criminal pode ser aplicada, sem que antes desse mesmo fato exista uma lei prevendo tal conduta como crime, estabelecendo ainda a respectiva pena para esta". Tal frase define qual dos princípios abaixo?

a) Presunção de inocência.

b) Autorregulamentação.

c) Ubiquidade.

d) Reserva legal.

e) Territorialidade.

3. A concepção atual do princípio da legalidade é obtida no quadro da denominada função de garantia da lei penal que provoca desdobramento do princípio em exame em quatro outros princípios. Assinale a alternativa que NÃO apresenta um desses princípios:

a) *Lex certa.*

b) *Lex praevia.*

c) *Lex mercattoria.*

d) *Lex scripta.*

e) *Lex stricta.*

Seção 4.2

Crimes praticados por meio eletrônico

Diálogo aberto

Na última seção, estudamos alguns conceitos básicos próprios do Direito Penal, bem como propomos a aplicação destes à realidade tecnológica atual. Nesta seção, iremos apresentar as principais condutas que podem se evidenciar por meio de uma ou mais técnicas computacionais, analisando ainda se a legislação brasileira define ou não uma punição específica, de modo a atender o princípio da reserva legal.

Retomando brevemente nossa situação geradora de aprendizagem (SGA), temos que você foi contratado por uma empresa na área de tecnologia da informação para o cargo de analista de segurança da informação. Você teve a ideia de realizar um "teste de penetração" (pentest), simulando o ataque de uma fonte maliciosa. Todavia, para tornar o teste o mais realista possível, você avisou somente seu superior hierárquico. Uma vez executado o teste, ele gerou o caos entre diversos setores, que ficaram contrariados com o pânico momentâneo causado.

Consideremos a seguinte situação-problema: se no decorrer do teste de penetração, por acidente, algumas informações forem destruídas, tal fato configuraria algum crime eletrônico?

Para resolvermos esta questão, iremos estudar as diversas condutas que configuram crimes eletrônicos, analisando aquelas que se enquadram tanto no conceito de delito informático próprio, quanto de delito informático impróprio. Como sabemos, estes são conceitos tratados na seção anterior, que dizem respeito justamente à classificação dos crimes informáticos, sob uma perspectiva doutrinária ou acadêmica. Por sua vez, nesta seção iremos aprofundar tais estudos, de modo a analisar as espécies de crimes que se encaixam em cada um desses gêneros, desde as clássicas e recorrentes fraudes eletrônicas, até crimes recentemente incorporados à nossa legislação, como a invasão de dispositivo informático.

Não pode faltar

Levando em conta que o computador e a internet podem ser utilizados enquanto instrumentos para a prática de crimes "comuns", iremos discorrer sobre alguns dos principais delitos que permitem ser perpetrados por esses meios, e que, consequentemente, adequam-se ao conceito de delitos informáticos impróprios, conforme estudamos na Seção 4.1. Após, iremos analisar brevemente as condutas que se amoldam ao conceito de delitos informáticos próprios.

Posto isso, passamos para a análise das principais condutas que podem ser classificadas como **delitos informáticos impróprios**, ou seja, aqueles cujo bem jurídico violado não é necessariamente um "sistema informático", mas que o computador ou a internet são meios para violação de outro bem juridicamente protegido, como patrimônio, honra, sigilo etc.

Assimile

Aos delitos em que o computador foi instrumento para a execução do crime, mas não houve ofensa ao bem jurídico "inviolabilidade de informações automatizadas", denominamos delitos informáticos impróprios.

a) Crimes contra o patrimônio em geral

A modalidade que talvez seja a de maior preocupação é a dos que lesam o patrimônio das pessoas físicas ou jurídicas. Dentre muitos, podemos destacar o furto, o dano e a extorsão. Um dos crimes de maior alcance é aquele em que os criminosos transferem dinheiro de contas de terceiros para suas próprias contas, ou de terceiros para depois se apoderarem da quantia. Tal conduta poderia se amoldar, dependendo do caso concreto, ao crime de estelionato ou ao crime de furto. Igualmente, temos que inutilizar ou deteriorar coisa alheia amolda-se ao tipo penal descrito no crime de dano, no entanto, existem divergências em saber se, por exemplo, um bit por ser considerado tangível e sofrer um dano visível. Ao nosso ver, o crime de dano previsto no art. 163 do Código Penal Brasileiro é perfeitamente aplicável à tutela dos dados informáticos, tratando-se de interpretação extensiva da palavra "coisa", elemento objetivo do tipo penal. A proteção patrimonial dos dados não se limita a seu valor econômico, pois a intenção do legislador foi proteger todo patrimônio da vítima, compreendido não só como tutela de valores econômicos, mas também do valor-utilidade e do valor afetivo que porventura tenha a coisa.

Já o crime de extorsão ganhou destaque recentemente em razão da prática do *ransomware* ou "sequestro de dados", em que o criminoso criptografa o banco de dados de determinada pessoa e, posteriormente, exige o pagamento de uma

quantia em dinheiro para revelar a chave de decriptação.

b) Fraudes em geral

As fraudes de maior frequência na internet ocorrem em leilões, compra e venda de mercadorias, pirâmides, trabalhos em casa com promessas de altos ganhos, utilização de senhas falsas ou alheias na conexão com provedores de acesso ou aplicação. As fraudes amoldam-se normalmente ao tipo penal descrito no artigo 171 do Código Penal, que tipifica o crime de estelionato. O estelionato pode ser praticado por qualquer meio eleito pelo sujeito ativo do crime, inclusive pela internet.

Exemplificando

Um exemplo clássico de fraude eletrônica refere-se ao golpe denominado "arara virtual", em que o sujeito cria um site de comércio eletrônico para a venda de produtos diversos, ofertando-os a preços convidativos, mediante o depósito do valor em conta bancária.

c) Crimes contra a honra

São atos que denigrem a integridade moral das pessoas via calúnia, injúria ou difamação, utilizando-se a internet como instrumento para potencialização da divulgação das ofensas, podendo ser praticado com uso de mensagens, dizeres, imagens etc. O Código Penal brasileiro prevê os crimes contra a honra nos artigos 138 e seguintes. Tais crimes, quando praticados pela internet, podem provocar às vítimas danos em extensão bem maior do que se praticados nas vias ordinárias da vida real. Isso porque uma informação circulando na rede e/ou colocada em redes sociais alcança um número ilimitado de pessoas, em razão da "ampliação" do espaço público, por onde os efeitos do crime poderiam percorrer.

d) Racismo

O racismo é a divulgação da aversão a determinados grupos de pessoas, muitas vezes incitando à violência, seja pela etnia, pela religião, pela nacionalidade, podendo se dar, assim como os crimes contra a honra, por meio das redes sociais, sites, e-mails etc. No Brasil, há uma lei específica sobre o assunto (Lei nº 7.716/1989), que define os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. De acordo com o artigo 20 da citada Lei, é crime "praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional". Acontece que, se o crime for praticado por intermédio dos meios de comunicação social ou publicação de qualquer natureza, o juiz poderá determinar a cessação das respectivas transmissões eletrônicas ou a interdição das mensagens ou páginas na rede mundial de computadores.

e) Interceptação de correspondência

Trata-se da direta afronta ao preceito constitucional do sigilo à correspondência, sendo o ato de interceptar uma correspondência dirigida a certa pessoa. Nosso Código Penal prevê no artigo 151 que "devassar indevidamente o conteúdo da correspondência fechada, dirigida a outrem, é crime. Na internet, a interceptação de correspondência pode se dar pela violação de e-mail ou outro tipo de comunicação em que somente o destinatário deveria receber a mensagem com exclusividade. A violação pode se dar pela leitura, modificação, ou uso dos dados contidos na mensagem.

f) Pornografia infantil

A pornografia infantil talvez seja o crime que mais provoque a repulsa da sociedade. Não há qualquer forma de se aceitarem as situações constrangedoras a que crianças são submetidas. Não se pode confundir pornografia infantil com pedofilia. A pornografia infantil é crime previsto no Estatuto da Criança e Adolescente (Lei nº 8.069/1990). Já a pedofilia é uma anomalia (doença), na qual seu portador sente-se atraído sexualmente por crianças. Os principais dispositivos que tipificam o crime de pornografia infantil são os artigos 240 e 241 do citado Estatuto da Criança e do Adolescente.

g) Crimes contra a propriedade intelectual

Por fim, temos os crimes praticados contra a propriedade intelectual de terceiros. O Código Penal, em seu artigo 184, prevê pena específica para quem viola direitos autorais de terceiros. Na internet, tal violação se dá de diversas maneiras, desde a disponibilização de conteúdo protegido por direito de autor em sites e redes sociais, até a pirataria de softwares. Além do Código Penal, existem crimes específicos também previstos na Lei de Propriedade Industrial (Lei nº 9.279/1996), como os crimes de concorrência desleal e violação de marca.

Faça você mesmo

Caso tenha conhecimento de algum crime eletrônico, principalmente se considerado como delito informático impróprio, denuncie na ferramenta da "Safernet", um dos principais órgãos responsáveis por registrar tais estatísticas. Disponível em: <http://new.safernet.org.br/denuncie>. Acesso em: 10 out. 2016.

Uma vez vistas as principais condutas que podem ser consideradas crimes informáticos impróprios, passamos para a análise daquelas em que o bem jurídico "informática" e agredido, ou seja, passamos para a análise dos **delitos informáticos próprios**.

Assimile

Os delitos em que os bens jurídicos afetados foram a "inviolabilidade de informações automatizadas", denominamos delitos informáticos próprios.

a) Invasão de dispositivos informáticos

Tal ação passou a ser considerada crime em razão do acréscimo do art. 154-A ao Código Penal, por meio da Lei nº 12.737/2012, a chamada "Lei Carolina Dieckmann". Tal delito consiste em invadir dispositivo informático alheio, conectado ou não à rede de computadores, por meio da violação indevida de mecanismo de segurança e com o objetivo de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, ou ainda, instalar vulnerabilidade para obter vantagem ilícita. Neste primeiro momento, iremos nos ater à tipificação do crime em si, sendo que na Seção 4.3 iremos estudar o tipo penal aqui descrito de maneira detalhada a fim de apontar falhas e polêmicas.

b) Interrupção de serviço informático/telemático

De acordo com os ajustes providos pela citada Lei nº 12.737/2012 ao Código Penal, o artigo 266 deste diploma jurídico passou a ter nova redação. Assim, quem interrompe serviço telemático ou de informação de utilidades pública, ou mesmo impede ou dificulta-lhe o restabelecimento, pratica referido tipo penal. Trata-se de verdadeira punição por ataques DoS (*Denial of Service*) praticados em face de sites públicos, algo que se tornou muito comum no Brasil, principalmente como forma de protesto por grupos de *hacktivistas*.

c) Clonagem/ falsificação de cartão de crédito e débito

O legislador brasileiro optou por tipificar tal conduta, que anteriormente era tratada como crime informático impróprio, sustentado pelo artigo 155 do Código Penal (Furto). Neste caso, a clonagem do cartão fica equiparada à falsificação de documento particular. Como a aplicação do art. 155 era polêmica, resolveu-se coibir esta prática tão comum em nosso país por meio de um tipo penal específico e expresso.

Reflita

Como vimos, várias condutas delituosas que utilizam o meio eletrônico como ferramenta para sua prática possuem previsão específica em nossa legislação. Por outro lado, tipos penais que visam proteger a "informática" ou um "sistema de informações" ainda são incipientes em

nosso país. Isso demonstra que o legislador brasileiro ainda não possui maturidade suficiente para perceber a periculosidade de tais condutas? Afinal, o que é mais perigoso, um assassino com uma arma em punho ou um cracker que pode provocar um incidente numa usina nuclear?

O Brasil, em termos de legislação, ainda está atrasado se comprado com outros países que, por exemplo, usam como diretriz a Convenção de Budapeste sobre cibercrimes para criar normas próprias e específicas para combater esse tipo de delito. Todavia, é importante que um país, ao criar normas desta estirpe leve em consideração a liberdade de expressão e outros direitos conquistados pelos usuários da internet, sob pena de engessar o espaço virtual e desvirtuar a internet como instrumento de interação global. A dificuldade é claramente achar um ponto de equilíbrio entre a impunidade e a restrição de direitos individuais.

Pesquise mais

O inteiro teor da Convenção de Budapeste sobre cibercrimes pode ser acessada através do endereço eletrônico <http://www.internacional.mpf.mp.br/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf>. Repare nas disposições relacionadas à preservação de provas e cooperação multinacional. Levando em consideração o elemento "territorialidade" estudado na Seção 1.1, consideramos relevante a troca de informações entre órgãos investigativos internacionais.

Sem medo de errar

Vamos retomar nossa situação-problema? Se no decorrer do teste de penetração, por acidente, algumas informações forem destruídas, tal fato configuraria algum crime eletrônico?

Atenção

A modalidade que talvez seja a de maior preocupação é a dos que lesam o patrimônio das pessoas físicas ou jurídicas. Dentre muitos, podemos destacar o furto, o dano e a extorsão.

Conforme estudamos, caso a conduta praticado por um sujeito ativo leve à inutilização ou deterioração de coisa alheia, poderíamos estar diante do tipo penal descrito no crime de dano, previsto no artigo 163 do Código Penal. No entanto, existem divergências em saber se, por exemplo, um bit por ser considerado tangível

e sofrer um dano visível. Ao nosso ver, o crime de dano previsto no art. 163 do Código Penal Brasileiro é perfeitamente aplicável à tutela dos dados informáticos, tratando-se de interpretação extensiva da palavra "coisa", elemento objetivo do tipo penal. A proteção patrimonial dos dados não se limita a seu valor econômico, pois a intenção do legislador foi proteger todo patrimônio da vítima, compreendido não só como tutela de valores econômicos, mas também do valor-utilidade e do valor afetivo que porventura tenha a coisa.

Avançando na prática

Ataques de negação de serviço e o Código Penal

Descrição da situação-problema

Você, ainda na condição de analista de segurança da informação de determinada empresa, é surpreendido no meio da madrugada por um alerta de que o site oficial da empresa está sofrendo um ataque de negação de serviço, tornando tal página indisponível para todos os usuários. Feito o contingenciamento do incidente, o diretor da empresa pergunta se seria possível registrar um boletim de ocorrência na Delegacia de Combate a Crimes Cibernéticos mais próxima, Pergunta-se: a conduta praticada contra a empresa poderia se enquadrar em algum dos tipos penais estudados?

Lembre-se

O Código de Processo Penal prevê como sendo um tipo penal a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.

Resolução da situação-problema

Conforme estudado, de acordo com os ajustes providos pela citada Lei nº 12.737/2012 ao Código Penal, o artigo 266 deste diploma jurídico passou a ter nova redação. Assim, quem interrompe serviço telemático ou de informação de utilidades pública, ou mesmo impede ou dificulta-lhe o restabelecimento, pratica referido tipo penal. Trata-se de verdadeira punição por ataques DoS (*Denial of Service*) praticados em face de sites públicos, algo que se tornou muito comum no Brasil, principalmente como forma de protesto por grupos de *hacktivistas*. No caso em tela, temos que o website da empresa é um site privado, não enquadrando-se na categoria de "serviço telemático de utilidade pública", conforme prevê o tipo penal descrito no artigo 266. Assim, a conduta praticada contra a empresa não se enquadra no referido tipo penal.

Faça você mesmo

Para saber mais sobre os ataques DoS ou DDoS e sua criminalização no Brasil, sugerimos a leitura do artigo do Prof. Marcelo Crespo no endereço <http://canalcienciascriminais.jusbrasil.com.br/artigos/229897612/ataques-dos-e-ddos-anotacoes-em-face-do-ordenamento-juridico-penal-brasileiro>. Acesso em: 4 out. 2016.

Faça valer a pena

1. A prática do *ransomware* ou "sequestro de dados", quando o criminoso criptografa o banco de dados de determinada pessoa e, posteriormente, exige o pagamento de uma quantia em dinheiro para revelar a chave de decriptação, pode ser enquadrado em qual dos tipos penais abaixo?

a) Dano.

b) Furto.

c) Roubo.

d) Extorsão.

e) Fraude.

2. O golpe denominado "arara virtual", em que o sujeito cria um site de comércio eletrônico para a venda de produtos diversos, ofertando-os a preços convidativos, mediante o depósito do valor em conta bancária, pode ser enquadrado em qual dos tipos penais abaixo?

a) Roubo.

b) Fraude.

c) Dano.

d) Extorsão.

e) Furto.

3. Considere as seguintes afirmativas:

I – Crimes contra a honra são atos que denigrem a integridade moral das pessoas via calúnia, injúria ou difamação, que podem utilizar a internet como instrumento para potencialização da divulgação das ofensas.

II – O Código Penal brasileiro não prevê o uso da internet para prática dos crimes contra a honra, não sendo possível, consequentemente, punir eventuais agressores.

III – Tais crimes, quando praticados pela internet, podem provocar às vítimas danos em extensão bem maior do que se praticados nas vias ordinárias da vida real. Isso porque uma informação circulando na rede e/ou colocada em redes sociais alcança um número ilimitado de pessoas.

Estão corretas as afirmativas:

a) I, apenas.

b) I e II.

c) II e III.

d) I e III.

e) I, II e III.

Seção 4.3

Novos tipos penais e a lei Carolina Dieckmann

Diálogo aberto

Na Seção 4.2 aprofundamos nossos estudos sobre os crimes eletrônicos, de modo a analisar detalhadamente as condutas consideradas crimes informáticos próprios e impróprios. Entre os crimes informáticos próprios, analisamos três tipos penais distintos, que foram incluídos em nossa legislação penal através da Lei nº 12.737/2012, conhecida também como "Lei Carolina Dieckmann". Nesta seção iremos detalhar ainda mais esses tipos penais, analisando de maneira crítica os erros e acertos do legislador brasileiro, bem como estudaremos algumas situações práticas em que a aplicação da Lei ainda é motivo de discussão pela doutrina.

Para tanto, vamos retomar brevemente nossa Situação Geradora de Aprendizagem (SGA): Você foi contratado por uma empresa na área de tecnologia da informação para o cargo de analista de segurança da informação. Uma de suas atribuições é analisar e medir o nível de capacitação dos funcionários e colaboradores acerca dos riscos de segurança da informação, como vazamento de dados, disseminação de códigos maliciosos, entre outros. Para tanto, você teve a ideia de realizar um "teste de penetração" (pentest), simulando o ataque de uma fonte maliciosa. Todavia, para tornar o teste o mais realista possível, você avisou somente seu superior hierárquico. Uma vez executado o teste, o mesmo gerou o caos entre diversos setores, que ficaram contrariados com o pânico momentâneo causado.

Para esta Seção 4.3, considere a seguinte situação-problema: Após a realização do pentest conforme descrito na SGA, é convocada uma reunião, de modo que um dos diretores indaga a você: a prática pode ser enquadrada no artigo 154-A do Código Penal, que prevê o crime de "invasão de dispositivo informático?

Para responder a esta questão iremos analisar de maneira detalhada as peculiaridades trazidas pelo tipo penal previsto no artigo 154-A, analisando sua aplicabilidade em alguns casos práticos, bem como apontando os erros e acertos do legislador. Igualmente, iremos estudar os outros dois tipos penais incluídos pela Lei Carolina Dieckmann em nosso ordenamento jurídico penal, fazendo também uma análise mais crítica.

Não pode faltar

A cópia indevida de dados ou informações no Brasil era conduta sem tipo associado. Conforme estudamos nas seções anteriores, muitos promotores, em tais casos, ofereciam denúncia em face do crime de furto, previsto no artigo 155 do Código Penal. Na doutrina, muitos asseveraram ser impossível a aplicação do tipo, considerando que a coisa "dados" não saía da esfera de disponibilidade da vítima, mas tão somente era "copiada". Tal lacuna existente na legislação criminal foi suprida com a Lei nº 12.737/2012, conhecida como "Lei Carolina Dieckmann", especificamente no artigo 154-A do Código Penal. Referida Lei surgiu a partir de um incidente envolvendo a atriz da Rede Globo de televisão, que foi vítima de obtenção indevida de imagens contidas em sistema informático de natureza privada, e cujo episódio acabou acelerando o andamento de projetos que já tramitavam com o fito de regulamentar essas práticas invasivas perpetradas em meios informáticos.

Assimile

A Lei nº 12.737, de 30 de novembro de 2012, trouxe para o ordenamento jurídico-penal brasileiro três importantes alterações: a inclusão do tipo penal "invasão de dispositivo informático"; inclusão de serviços telemáticos no crime de "interrupção de serviços telegráfico ou telefônico"; e a equiparação de cartões de crédito e débito para fins do crime de "falsificação de documento particular".

Vejamos o que dispõe aludido artigo:

"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 obtidos.
§ 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".

Em que pese a intenção do legislador de inovar o arcabouço de normas penais, a criação do tipo penal citado trouxe algumas críticas por parte de juristas e operadores do direito, tendo em vista a conduta descrita possuir algumas expressões um tanto quanto vagas ou de dúbia interpretação, o que não é desejável para conduta considerada um tipo penal. Destacamos aquelas que consideramos como as mais graves.

Primeiramente, iremos analisar a questão daquilo que pode ser considerado mecanismo de segurança ou não. Como vimos, é indispensável que o ativo a ser invadido esteja protegido por mecanismo de segurança ou barreira tecnológica. Em segurança da informação, mecanismos de segurança podem ser considerados "proteções" ou medidas que objetivam livrar a informação de situações que possam causar danos (JESUS; MILAGRE, 2016).

Exemplificando

As proteções podem ser "lógicas", como permissões em sistemas de arquivos, firewalls ou senhas, e sistemas de detecção de intrusos, físicas, como cofres, portas, fechaduras, e "administrativas", como políticas, normas e procedimentos de segurança da informação.

Para fins do disposto no artigo 154-A, entende-se que a proteção lógica é a única adequada para fins de enquadramento no tipo penal. Quanto às proteções administrativas, entendemos que elas não incorporam o conceito de "mecanismo de segurança", mas se assemelhando à "ausência de autorização" para a acesso a determinado dispositivo.

É justamente na "ausência de autorização" que reside outro ponto polêmico da norma penal. Como verificado, para que um agente seja responsabilizado pelo delito do art. 154-A, basta que o acesso se dê a um dispositivo contendo mecanismo de segurança, e que este acesso seja feito sem a autorização, expressa ou tácita, do titular do dispositivo.

Ocorre que a ausência de proibição expressa para acesso não significa autorização tácita para a sua invasão. A ausência de proibição expressa significa proibição tácita. Por outro lado, há casos em que se subtende a autorização tácita para invasão do dispositivo, sobretudo a depender da relação entre as partes envolvidas. Como exemplo, citamos a realização do pentest. Ora, a pessoa responsável pela segurança da informação e, consequentemente, responsável por realizar o teste de penetração, não precisa de autorização expressa ou tácita para tanto, já que tal atividade é intrínseca a suas funções.

O terceiro aspecto polêmico do novo tipo penal refere-se à invasão de dispositivos informáticos e a pescaria de senhas ou *phishing scam*. Caso um criminoso virtual induza sua vítima, por meio de técnicas de *phishing scam* (engenharia social), a lhe conceder acesso a seu computador, liberando portas de entrada e acessando conteúdos indevidamente, tal conduta poderia ser enquadrada no crime previsto no artigo 154-A?

Como vimos anteriormente, para que o crime de invasão de dispositivo informático seja configurado é necessário, entre outras coisas, que haja violação de mecanismo de segurança. Existem duas correntes que discutem tal questão. Para a primeira corrente, não haveria crime, tendo em vista que os acessos foram exitosos graças à própria ação e colaboração da vítima. Já a segunda corrente, qualquer modalidade de engenharia social enquadra-se no art. 154-A, tendo em vista que a fraude poderia ser considerada "instrumento de invasão", com a ressalva da possibilidade de um crime posterior, por exemplo, o estelionato. Ao nosso ver, considerar que no *phishing scam* ocorre a invasão de dispositivo informático, é assumir forçosamente que as pessoas (vítimas) são espécies de "mecanismos de segurança", pois, nesse caso, seriam elas as violadas, e não um "mecanismo de segurança" lógico, como um firewall ou uma senha.

Por fim, o último ponto polêmico, diz respeito à questão da invasão com fim único de dar uma "espiadinha" nos dados ou informações contidos no dispositivo. Ora, o tipo penal é claro ao dispor que somente ocorrerá o delito se a invasão for

realizada "com o fim de obter, adulterar ou destruir dados ou informações". E se da invasão não resultar a obtenção, adulteração ou destruição dos dados? Ao nosso ver, não é necessária a cópia dos dados para a prática do crime, bastando a invasão com a "intenção da obtenção dos dados". O problema é a demonstração dessa intenção, que só poderá ser provada por perícia técnica.

Pesquise mais

O crime de invasão de dispositivo informático foi muito bem abordado em artigo escrito pelo professor e delegado Eduardo Cabette. Disponível em: <http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>. Acesso em: 4 out. 2016.

Continuando nossos estudos sobre a Lei nº 12.737/2012, ela trouxe outras disposições que também alteraram o Código Penal, incluindo outros tipos penais, conforme estudamos na Seção 4.2, quais sejam, a "interrupção de serviço telemático ou de informação pública" e a "falsificação de cartão de crédito ou débito". Vejamos cada um:

> 1) 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.

Quanto à interrupção de serviços, não existem maiores críticas quanto a este tipo penal específico, salvo aquela referente a não previsão de aplicação do tipo aos casos de ataques de negação de serviço feitos a sites ou serviços particulares. A limitação do tipo a serviços e sites públicos deixou uma lacuna desnecessária. Nesse contexto, resta ao particular recorrer a outros tipos penais, como crime de dano.

> 2) 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.

Igualmente, em relação ao tipo penal falsificação de cartão de crédito e débito, percebemos falhas do legislador ao atrelar o tipo penal a uma tecnologia específica, no caso o uso de cartões de crédito e débito. E quando o cartão se extinguir? O legislador deixou a desejar na reflexão de tal dispositivo. Poderia equiparar os documentos eletrônicos ao particulares para fins de incidência do tipo penal. Basta lembrar que hoje temos documentos em DCs, pen drives, chips, HDs entre outros (JESUS; MILAGRE, 2016).

Em conclusão, temos que a Lei nº 12.737/2012, a chamada "Lei Carolina Dieckmann", foi um pequeno avanço em relação ao combate aos crimes eletrônicos. Como vimos, a redação utilizada pelo legislador está longe da perfeição, todavia, demonstra certa preocupação para este novo tipo de criminalidade. Caberá ao Judiciário aparar arestas na aplicação dos tipos penais aos casos concretos. Nesse sentido, tem-se também que é preciso também rever questões ligadas à prisão dos sujeitos ativos desses crimes, sendo preferencial a aplicação de penas envolvendo prestação de serviços de segurança da informação.

Ademais, cumpre esclarecer que nenhum combate sério aos crimes informáticos ou eletrônicos esgota-se no processo tipificador. Sem cooperação internacional, sem melhoria do aparelhamento policial e sem o aperfeiçoamento do profissional dos que operam nessa área, inclusive do ponto de vista jurídico (advogados, juízes e promotores) a simples existência de uma adequada tipificação não tem o menor significado prático e não basta para tutelar a sociedade contra tão lesiva atividade criminosa (ROZA, 2007).

Reflita

Além das medidas acima citadas, você consegue pensar em outras capazes de auxiliar a sociedade no combate aos crimes eletrônicos? Você acredita que a adoção de um padrão legislativo internacional é adequado, ou isso iria contra a soberania legislativa de cada país?

Sem medo de errar

Vamos resolver nossa situação-problema? Após a realização do pentest, conforme descrito na SGA, é convocada uma reunião, de modo que um dos diretores indaga você: a prática pode ser enquadrada no artigo 154-A do Código Penal, que prevê o crime de "invasão de dispositivo informático?

Atenção

Para que um agente seja responsabilizado pelo delito do art. 154-A, basta que o acesso se dê a um dispositivo contendo mecanismo de segurança, e que este acesso seja feito sem a autorização, expressa ou tácita, do titular do dispositivo.

Primeiramente, cumpre esclarecer que a ausência de proibição expressa para acesso não significa autorização tácita para a sua invasão. A ausência de proibição expressa significa, na verdade, a proibição tácita. Por outro lado, há casos em que se subtende uma autorização tácita para invasão do dispositivo, sobretudo a depender da relação entre as partes envolvidas. No caso descrito tanto na SGA quanto na situação-problema, temos que o cargo ocupado, qual seja, analista de segurança da informação, pressupõe a autorização da empresa ou superiores hierárquicos para efetuar testes cujo objetivo sejam, justamente, avaliar o nível de segurança da informação da empresa. Ora, a pessoa responsável pela segurança da informação e, consequentemente, responsável por realizar o teste de penetração, não precisa de autorização expressa ou tácita para tanto, já que tal atividade é intrínseca a suas funções. Diferente seria, se existisse alguma norma específica, seja no contrato de trabalho, seja na Política de Segurança da Informação, exigindo autorização expressa de um superior hierárquico ou de uma diretoria ou comitê para executar o aludido teste de penetração.

Avançando na prática

Invasão de dispositivo informático e o phishing scam

Descrição da situação-problema

Você foi induzido por um criminoso virtual a lhe conceder acesso a seu computador particular, liberando portas de entrada e acessando conteúdos indevidamente, por meio de técnicas de phishing scam (engenharia social). Pergunta-se: tal conduta poderia ser enquadrada no crime previsto no artigo 154-A?

Lembre-se

Para que uma conduta seja enquadrada no crime previsto no artigo 154-A, é necessário que haja a violação de um "mecanismo de segurança".

Resolução da situação-problema

Como vimos anteriormente, para que o crime de invasão de dispositivo informático seja configurado é necessário, entre outras coisas, que haja violação de mecanismo de segurança. Existem duas correntes que discutem tal questão. Para a primeira corrente, não haveria crime, tendo em vista que os acessos foram exitosos graças à própria ação e colaboração da vítima. Já a segunda corrente, qualquer modalidade de engenharia social enquadra-se no art. 154-A, tendo em vista que a fraude poderia ser considerada "instrumento de invasão", com a ressalva da possibilidade de um crime posterior. A nosso ver, considerar que no phishing scam ocorre a invasão de dispositivo informático, é assumir forçosamente que as pessoas (vítimas) são espécies de "mecanismos de segurança", pois, nesse caso, seriam elas as violadas, e não um "mecanismo de segurança" lógico, como um firewall ou uma senha.

Faça você mesmo

Para saber mais sobre engenharia social, prática cada vez mais comum, inclusive no ambiente interno de empresas, sugerimos a leitura do artigo disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>. Acesso em: 4 out. 2016.

Faça valer a pena

1. A cópia indevida de dados ou informações no Brasil era conduta sem tipo associado. Diante desse cenário, muitos promotores, em tais casos, ofereciam denúncia em face de qual crime?

a) Estelionato.

b) Injúria.

c) Dano.

d) Furto.

e) Roubo.

2. Assinale a alternativa que apresenta um exemplo de um novo tipo penal criado pela Lei nº 12.737/2012 (Lei Carolina Dieckmann)?

a) Sequestro de dados.

b) Invasão de dispositivo informático.

c) Furto de dados.

d) Criação de perfil falso em redes sociais.

e) Pornografia de vingança.

3. De acordo com o artigo 154-A do Código Penal, é crime "invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de _____ 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". Complete a lacuna com a expressão correta:

a) Firewall.

b) Mecanismo de criptografia.

c) Mecanismo de segurança.

d) Criptografia.

e) Antivírus.

Seção 4.4

Controvérsias envolvendo crimes eletrônicos

Diálogo aberto

Na Seção 4.3, estudamos os novos tipos penais e a Lei Carolina Dieckmann. Você deve se lembrar de que levantamos algumas questões polêmicas acerca do delito de invasão de dispositivo informático, como a realização do pentest por funcionário encarregado da segurança da informação de uma empresa. Pois bem. Nesta Seção 4.4 iremos analisar outras questões controversas, entretanto, sob um prisma mais genérico, que tem a ver com a "parte geral" do Código Penal, ou seja, aquela que se relaciona a própria aplicação da Lei Penal no tempo e no espaço. Igualmente, veremos algumas questões específicas sobre os crimes contra o sistema financeiro e contra a propriedade intelectual.

Mas antes, vamos retomar nossa situação geradora de aprendizagem (SGA): você foi contratado por uma empresa na área de tecnologia da informação para o cargo de analista de segurança da informação. Uma de suas atribuições é analisar e medir o nível de capacitação dos funcionários e colaboradores acerca dos riscos de segurança da informação, como vazamento de dados, disseminação de códigos maliciosos, entre outros. Para tanto, você teve a ideia de realizar um "teste de penetração" (pentest), simulando o ataque de uma fonte maliciosa. Todavia, para tornar o teste o mais realista possível, você avisou somente seu superior hierárquico. Uma vez executado o teste, ele gerou o caos entre diversos setores, que ficaram contrariados com o pânico momentâneo causado.

A partir da SGA, propomos a seguinte situação-problema: partindo do pressuposto que para realizar o pentest você utilizou um proxy de modo a mascarar a origem do ataque, e que este proxy está localizado em Singapura. Na hipótese de algum diretor decidir puni-lo pela falta de aviso na realização do teste, propondo uma ação penal com base no artigo 154-A do Código Penal (invasão de dispositivo informático), qual o juízo competente para processar e julgar a ação?

Para responder a estas e outras questões, iremos estudar algumas questões controversas sobre o direito penal informático, tais como o tempo do crime, a competência e lugar do crime informático, o concurso de pessoas, bem como outras controvérsias envolvendo condutas específicas, como os crimes contra o sistema financeiro e contra a propriedade intelectual.

Não pode faltar

Conforme dito acima, os crimes informáticos possuem algumas questões controversas, que dificilmente são objeto de unanimidade na doutrina e na jurisprudência. Vejamos algumas delas.

1) Tempo do crime

A fixação do instante em que o crime foi praticado é importante sob vários aspectos, principalmente para determinar a lei vigente no momento em que o delito se consumou, no caso de sucessão de leis penais, para aferir a inimputabilidade penal, isto é, se o agente tinha 18 anos na ocasião da consumação, ou se ao tempo da ação ou omissão era inteiramente incapaz de entender o caráter ilícito do fato, ou ao menos se determinar de acordo com esse entendimento, além do exame de circunstâncias do crime e aplicação de eventual anistia condicionada no tempo.

A doutrina regulamentou a matéria enfocando três teorias: a) da atividade, para quem o crime se consuma com a prática da conduta, isto é, no momento da ação ou omissão; b) do resultado, para quem se considera tempo do crime o momento de seu resultado; e c) mista, para quem considera que o tempo do crime é tanto o momento da conduta quanto do resultado.

Assimile

Com a reforma penal de 1984, o legislador adotou em nosso Código Penal a teoria da atividade, de forma que considera tempo do crime o momento da ação ou omissão do agente, ou seja, no momento da prática da conduta prevista na norma penal incriminadora.

2) Competência e lugar do crime informático

A questão da territorialidade possui relativa controvérsia dentro da doutrina. Determinar a territorialidade implica determinar o juiz competente para processar e julgar um delito informático. Pontua-se que o Direito Penal brasileiro está relacionado ao território nacional, e o que se procede fora de tais limites resulta em revisão dos acordos entre países. No Brasil, a legislação que norteia a questão está relacionada nos artigos 5º, 6º e 7º do Código Penal.

No tocante ao local do crime, o Código Penal adotou, em seu artigo 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. Deste modo, o considerar alguém, no Estado de Minas Gerais, que invade o computador de outrem, localizado em São Paulo, teríamos o juízo onde está o dispositivo invadido como competente para julgar o delito informático.

Por outro lado, no que tange às condutas ilícitas praticadas em território estrangeiro, não se aplicariam, em regra as normas brasileiras, considerando a soberania do país, sendo que a questão normalmente é tratada pela extradição.

Vocabulário

Extradição é um instrumento jurídico, através do qual, um Estado (requerido) soberanamente entrega à justiça criminal de outro Estado (requerente) uma pessoa, porquanto este último tem jurisdição para processá-lo e julgá-lo (extradição processual) ou aplicar-lhe uma sanção penal (extradição executiva) (ARROS LIMA, 2002, p. 13). Ou seja, a extradição é o processo oficial pelo qual um Estado solicita e obtém de outro a entrega de uma pessoa condenada ou suspeita da prática de uma infração criminal.

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 este agente adentre no território nacional. Logo, crimes cometidos por meio de proxies, VPNs, entre outros recursos para mascarar a origem da conexão, em que o agente está no Brasil e só vale de uma conexão no exterior, podem ser processados aqui, desde que, claro, identificado o criminoso. Justamente aí que reside mais um problema, pois provedores estrangeiros, muitas vezes, se recusam a fornecer dados de acesso a aplicações feitas por brasileiros, mas armazenados no exterior, tendo em vista que, em regra, a legislação brasileira não se aplicaria ao país onde tais provedores estão sediados.

Importante ainda esclarecer que, nos termos do § 2º do artigo 70 do Código de Processo Penal, quando os atos executórios tenham ocorrido fora do Brasil, a competência será do local onde a infração se deu ou foi concluída a ação delituosa. Pondera-se, no entanto, que, em se tratando de crimes praticados por brasileiros no exterior que façam vítimas no Brasil, por questões de soberania, a conduta praticada pelo agente deve ser considerada ilícita em ambos os países, bem como deverá o agente ingressar em território nacional para que seja processado.

3) Concurso de pessoas

O concurso de pessoas pode ser definido como a cooperação desenvolvida por mais de uma pessoa para a prática de um ilícito penal. Significa, na realidade, a prática de um ilícito penal por duas ou mais pessoas. Importa ainda, fazermos uma breve distinção entre coautoria e participação.

Considera-se coautor aquele que pratica, de algum modo, a figura típica. Ou seja, ele realiza diretamente a ação (ou verbo) prevista no tipo penal (ex.: "matar" alguém). Por sua vez, ao partícipe fica reservada a posição de auxílio material

ou suporte moral (incluindo o induzimento, instigação ou comando) para a concretização do crime; ele não realiza diretamente o verbo que descreve a conduta criminal, ele não ingressa no tipo penal.

O julgador do caso pode aplicar pena igual ao coautor e ao partícipe, bem como pode aplicar pena menor ao partícipe, desde que seja recomendável. Para a punição do partícipe, deve o autor ter praticado um fato típico.

Transpondo esse raciocínio para nosso objeto de estudo, percebemos que o concurso de pessoas é possível, por exemplo, no caso de desvio de importâncias de contas bancárias em que haja o uso da internet, quer na forma de coautoria, quer na forma de participação.

Exemplificando

Quando o agente, intencionalmente, empresta a sua conta bancária para receber o dinheiro subtraído eletronicamente da vítima e posteriormente saca e entrega a um cracker, concorreu para a prática do crime, devendo responder como coautor.

Vale observar, no entanto, que, se o beneficiário não tiver a intenção de participar da subtração do dinheiro, mas tão somente, ceder sua conta bancária para receber o dinheiro ilícito, deverá, em tese, ser responsabilizado pelo crime de receptação, previsto no tipo penal descrito no artigo 180 do Código Penal. Para tanto, se faz necessário que tenha conhecimento da origem ilícita do dinheiro.

4) Crimes contra o sistema financeiro

Existem alguns julgados que têm tratado o furto mediante fraude praticado por meio da internet, também como delito de violação de sigilo bancário. Todavia, o sujeito ativo deste delito, previsto no artigo 10 da Lei Complementar nº 105/2001, é aquele que, em razão do seu ofício, viola sigilo operação ou serviço prestado por instituição financeira de que tenha conhecimento. Ou seja, aquele que tem acesso às informações sigilosas sobre operações ou serviços prestados pela instituição financeira é quem poderá praticar o crime de violação de sigilo bancário.

Como se percebe, não se pode incluir o delito de quebra de sigilo nos casos de furto mediante fraude por meio da internet, uma vez que, em quase sua totalidade, apresentam sujeitos ativos sem a citada qualidade especial, salvo se ocorrer participação de pessoas que tenham acesso a tais informações bancárias em razão do ofício.

5) Crimes contra a propriedade intelectual

Conforme estudamos na Unidade 3, a internet é um campo fértil para a prática

de crimes contra a propriedade intelectual, com destaque para as violações de direitos autorais, marcas além da concorrência desleal. Todavia, cabe aqui levantar uma questão polêmica referente ao uso não comercial dos conteúdos protegidos por direito autoral ou por direito de propriedade industrial. Ora, será que o uso mínimo de um conteúdo protegido por direito de autor deveria ser considerado uma violação? Não poderiam existir exceções à regra? A verdade é que no Brasil, país que adota o sistema de proteção da propriedade intelectual conforme o modelo mais rígido e pessoal usado na Europa Continental, qualquer uso indevido pode ser considerado uma violação e até mesmo crime. Diferentemente, nos países de tradição anglo-saxã, o aspecto econômico é levado em consideração para analisar se determinado conteúdo foi, ou não, utilizado de maneira indevida. Trata-se da teoria do *fair use* ou "uso justo". Neste, analisa-se o tamanho do trecho da obra que foi utilizado, o aspecto (não) comercial da utilização, o impacto econômico causado pela utilização da obra nos valores a serem recebidos pelo autor ou criado, entre outros fatores.

Reflita

Na sua opinião, nossa legislação deveria fazer uma exceção para o uso mínimo, ou "uso justo" de uma obra protegida por direito de propriedade intelectual? Um exemplo de "uso justo" seriam os populares vídeos em que uma pessoa joga determinado jogo de videogame, fazendo comentários ao longo do jogo. Essa iniciativa foi encampada pela gigante Google, por meio do YouTube Gaming.

Mensagem final

Por fim, como mensagem final desta unidade, gostaríamos de reiterar que a criação de tipos penais específicos para o combate à criminalidade eletrônica não irá resolver o problema que nossa sociedade atualmente vive. Tal medida, se considerada de maneira isolada, não possui o condão de diminuir as crescentes ocorrências que testemunhamos em nosso cotidiano. Além dessas medidas outras são igualmente (ou mais) importantes. Entre elas destacamos o aparelhamento da polícia investigativa, que se encontra, muitas vezes, abandonada, em que pese a competência de seus profissionais; a conscientização de crianças, adolescentes e adultos de que a internet não é uma "terra sem lei" e que toda ação possui uma consequência; e ainda, a necessária cooperação entre organismos internacionais para facilitação de processos investigativos, tendo em vista o caráter global a ser considerado para prática desses crimes.

Pesquise mais

Outra ferramenta importante de combate ao cibercrime e, que vem ganhando cada vez mais força, é o uso da inteligência artificial. Neste artigo, entenda como um supercomputador pode ajudar a entender e reduzir ameaças. Disponível em: <http://computerworld.com.br/ibm-treinara-watson-para-combater-cibercrime>. Acesso em: 5 out. 2016.

Sem medo de errar

Vistos os principais conceitos, vamos resolver nossa situação-problema (SP): partindo do pressuposto que para realizar o pentest você utilizou um proxy de modo a mascarar a origem do ataque, e que este proxy está localizado em Singapura. Na hipótese de algum diretor decidir puni-lo pela falta de aviso na realização do teste, propondo uma ação penal com base no artigo 154-A do Código Penal (invasão de dispositivo informático), qual é o juízo competente para processar e julgar a ação?

Atenção

No tocante ao local do crime, o Código Penal adotou, em seu artigo 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.

Conforme estudado, a autoridade brasileira é competente para processar um crime digital praticado por agente brasileiro no exterior, com vítima no Brasil, mas dependerá que este agente adentre no território nacional. Logo, caso o crime seja cometido por meio de proxy pode ser processado aqui, desde que, claro, identificado o criminoso. Importante ainda esclarecer que, nos termos do § 2º do artigo 70 do Código de Processo Penal, quando os atos executórios tenham ocorrido fora do Brasil, a competência será do local onde a infração se deu ou foi **concluída a ação delituosa (resultado)**. Pondera-se, no entanto, que, em se tratando de crimes praticados por brasileiros no exterior que façam vítimas no Brasil, por questões de soberania, a conduta praticada pelo agente deve ser considerada ilícita em ambos os países, bem como deverá o agente ingressar em território nacional para que seja processado. Assim, apesar do uso de um servidor proxy localizado em Singapura, estando tanto o agente como a vítima localizados em território brasileiro, o juízo competente será o do Brasil, especificamente o do local de sede da empresa.

Avançando na prática

Tempo do crime informático

Descrição da situação-problema

Estudante do primeiro período do curso de ciência da computação, e entusiasta da cultura hacker, decide praticar suas "habilidades", invadindo o computador de uma ex-colega de colégio, de modo a obter determinadas fotos armazenadas em seu computador. Para tanto, ele utiliza um trojan, instalado no computador de sua colega. Com facilidade ele consegue obter tais fotos e as divulga na internet. Considerando que a instalação do vírus ocorreu às 23h58 do dia da véspera de seu aniversário de 18 anos, e a divulgação das fotos se deu à 01h43 do dia do seu aniversário de 18 anos, poderia João responder penalmente pelo crime previsto no artigo 154-A do Código Penal?

Lembre-se

Com a reforma penal de 1984, o legislador adotou em nosso Código Penal a teoria da atividade, de forma que considera tempo do crime o momento da ação ou omissão do agente, ou seja, no momento da prática da conduta prevista na norma penal incriminadora.

Resolução da situação-problema

A fixação do instante em que o crime foi praticado é importante sob vários aspectos, principalmente para determinar a lei vigente no momento que o delito se consumou, no caso de sucessão de leis penais, para aferir a inimputabilidade penal, isto é, se o agente tinha 18 anos na ocasião da consumação, ou se ao tempo da ação ou omissão era inteiramente incapaz de entender o caráter ilícito do fato, ou ao menos se determinar de acordo com esse entendimento, além do exame de circunstâncias do crime e aplicação de eventual anistia condicionada no tempo. A doutrina regulamentou a matéria enfocando três teorias: a) da atividade, para quem o crime se consuma com a prática da conduta, isto é, no momento da ação ou omissão; b) do resultado, para quem se considera tempo do crime o momento de seu resultado; e c) mista, para quem considera que o tempo do crime é tanto o momento da conduta quanto do resultado. Com a reforma penal de 1984, o legislador adotou em nosso Código Penal a teoria da atividade, de forma que considera tempo do crime o momento da ação ou omissão do agente, ou seja, no momento da prática da conduta prevista na norma penal incriminadora.

Assim, considerando que na data da "instalação da vulnerabilidade" no computador de sua ex-colega João tinha 17 anos, ele não responde penalmente

pelo crime previsto no artigo 154-A. Todavia, isto não quer dizer, por exemplo, que ele não responda civilmente pelos danos eventualmente causados em razão da divulgação das fotos da ex-colega na internet.

Faça você mesmo

A prática de cibercrimes e hacking por menores de idade não é algo incomum. O "castigo" aplicado a cada um deles pode ser diferente, como a condenação a ficar determinado período sem acessar a internet. Convidamos você a ler as seguintes histórias. Disponíveis em: <http://olhardigital.uol.com.br/fique_seguro/noticia/hacker-de-15-anos-e-condenado-a-seis-anos-sem-internet/30513> e <http://www.correiobraziliense.com.br/app/noticia/tecnologia/2014/10/08/interna_tecnologia,451444/com-apenas-13-anos-de-idade-hacker-mais-novo-da-china-diz-ser-bom-garoto.shtml>. Acesso em: 5 out. 2016.

Faça valer a pena

1. Qual das teorias referentes à definição do tempo do crime foi adotada pela doutrina e jurisprudência brasileiras?

a) Teoria do resultado.

b) Teoria da atividade.

c) Teoria Mista.

d) Teoria da ação.

e) Teoria da omissão.

2. De acordo com a teoria da atividade, considera-se o tempo do crime:

a) O momento da descoberta do crime.

b) O momento do resultado do crime.

c) O momento da prática da conduta prevista na norma penal incriminadora.

d) Tanto o momento da conduta quanto do resultado.

e) O momento do planejamentos dos atos executórios do crime.

3. Sobre a competência e lugar do crime informático, assinale a alternativa incorreta:

a) A questão da territorialidade possui relativa controvérsia dentro da doutrina.

b) Determinar a territorialidade implica determinar o juiz competente para processar e julgar um delito informático.

c) Pontua-se que o Direito Penal brasileiro, está relacionado ao território nacional, e o que se procede fora de tais limites resulta em revisão dos acordos entre países.

d) No Brasil, a legislação que norteia a questão está relacionada nos artigos 5º, 6º e 7º do Código Penal.

e) A fixação do local do crime é importante para aferir se o sujeito ativo tinha 18 anos à época da prática da conduta delituosa.

Referências

ARROS LIMA, Alberto Jorge Correia de. Extradição e direito internacional penal. **Revista da Escola Superior da Magistratura do Estado de Alagoas**, Maceió, v. 1, n. 1, p. 11-26, dez. 2002.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 19 ago. 2016.

_____. Decreto-lei nº 2.848, de 7 de dezembro de 1940. de 1940. Código Penal. **Diário Oficial da União**, Rio de Janeiro, RJ, 31 dez. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm>. Acesso em: 19 ago. 2016.

CABETTE, Eduardo. **O novo crime de invasão de dispositivo informático**. 2013. Disponível em: <http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crimeinvasao-dispositivo-informatico>. Acesso em: 4 out. 2016.

CARNEIRO, Adeneele Garcia. **Crimes virtuais**: elementos para uma reflexão sobre o problema na tipificação. 2012. Disponível em: <http://www.egov.ufsc.br:8080/portal/conteudo/crimes-virtuais-elementos-para-uma-reflex%C3%A3o-sobre-oproblema-na-tipifica%C3%A7%C3%A3o>. Acesso em: 4 out. 2016.

CERT.BR. **Códigos maliciosos** (Malware). Disponível em: <http://cartilha.cert.br/malware/>. Acesso em: 4 out. 2016.

CRESPO, Marcelo. **Ataques DoS e DDoS**: anotações em face do ordenamento jurídico penal brasileiro. 2015. Disponível em: <http://canalcienciascriminais.jusbrasil.com.br/artigos/229897612/ataques-dos-e-ddos-anotacoes-em-face-do-ordenamento-juridicopenal-brasileiro>. Acesso em: 4 out. 2016.

COMPUTERWORLD. **IBM treinará Watson para combater cibercrime**. 2016. Disponível em: <http://computerworld.com.br/ibmtreinara-watson-para-combater-cibercrime>. Acesso em: 5 out. 2016.

FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). **Direito e internet**: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. **Crimes na internet e inquérito policial eletrônico**. São Paulo: Edipro, 2012.

GOMES, Luiz Flávio. **Crimes informáticos**. 10 dez. 2000. Disponível em: <www.ibccrim.org.br>. Acesso em: 19 ago. 2016.

JESUS, Damásio Evangelista de. **Direito penal**: parte geral. São Paulo: Saraiva, 1993.

JESUS, Damásio E. de.; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

MINISTÉRIO PÚBLICO FEDERAL. **Convenção sobre o cibercrime**. 2001. Disponível em: <http://www.internacional.mpf.mp.br/normas-e-legislacao/legislacao/legislacoes-pertinentesdo-brasil/docs_legislacao/convencao_cibercrime.pdf>. Acesso em: 4 out. 2016

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

ROHRMANN, Carlos Alberto. **Curso de direito virtual**. Belo Horizonte: Del Rey: 2005.

ROZA, Fabrízio. **Crimes de informática**. 2. ed. Campinas: Bookseller, 2007.

RAFAEL, Gustavo de Castro. **Engenharia social**: as técnicas de ataques mais utilizadas. 2013. Disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>. Acesso em: 4 out. 2016.

SAFERNET. **Denuncie**. Disponível em: <http://new.safernet.org.br/denuncie>. Acesso em: 10 out. 2016.

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

TOLEDO, Francisco de Assis. **Princípios básicos de direito penal**. 4. ed. São Paulo: Saraiva, 1991.

VIANNA, Túlio Lima. **Fundamentos de direito penal informático**: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003.

ISBN 978-85-8482-700-8