DIREITO DIGITAL: O MARCO CIVIL BRASILEIRO DA INTERNET E AS INOVAÇÕES JURÍDICAS NO CIBERESPAÇO

DIGITAL RIGHTS: THE BRAZILIAN CIVIL RIGHTS INTERNET FRAMEWORK AND LEGAL INNOVATIONS IN THE CYBERSPACE

Roberto Renato Strauhs da Costa[1]
Fábio Pendiuk [2]

RESUMO

Recentemente, o tema do Direito Digital passou a ser tratado pelas grandes universidades do mundo como disciplina específica. Enquanto a especialidade do âmbito jurídico, se propõe a analisar o tratamento dado aos crimes praticados no ciberespaço. O debate ganha fôlego no Brasil, após os adventos do Marco Civil da Internet, da Lei Carolina Dieckmann e da Lei Azeredo, os quais regulam crimes dessa natureza. Em seus objetivos específicos, analisam o ambiente digital e suas consequências na prática de infração penal por internautas, suas responsabilidades civís/penais, a educação escolar tecnológica pautada na ética, os desafios da educação digital e, fundamentalmente, os princípios defendidos pelas leis n. 12.735/2012 e n. 12.737/2012, que estabelecem sanções penais para crimes digitais no país. Diante da atualidade e abrangência do tema, este artigo apresenta uma análise exploratória de publicações expoentes que compõem a bibliografia essencial para o debate contemporâneo sobre o Direito Digital e o Marco Civil da Internet.

Palavras-chave: Direito Digital, Marco Civil da Internet, Lei de Crimes Digitais.

ABSTRACT

Recently, the theme of Digital Rights came to be treated by the great universities as a specific discipline. As a legal specialty, it is proposed to analyze the treatment of crimes committed in cyberspace. The debate gains momentum in Brazil after the advent of the Brazilian Civil Rights Internet Framework, the Law Carolina Dieckmann and the Law Azeredo, which regulate crimes of this nature in the digital world. In their specific objectives, they analyze the digital environment and its consequences in the practice of criminal infraction by Internet users, the civil/criminal responsibility of those responsible, the ethical school education based on ethics, the challenges of digital education and fundamentally the principles defended by the laws number 12.735/2012 and n. 12.737/2012, which establish criminal sanctions for digital crimes in the country. Given the relevance of this topic, this article presents an exploratory analysis of exponent publications that compose the essential bibliography for the contemporary debate on the Digital Right and the Civil Framework of the Internet.

Keywords: Digital Rights, Brazilian Civil Rights Internet Framework, Cybercrime Law.

[1] Graduando do Curso de Bacharelado em Direito, da Faculdade de Educação Superior do Paraná (FESP), e-mail: <roberto.strauhs@gmail.com>.

[2] Doutor em Sociologia pela Universidade Federal do Paraná (UFPR), Professor Titular das disciplinas Sociologia Jurídica e Sociologia Geral do curso de Bacharelado em Direito, orientador do Grupo de Estudos em Sociedade & Direito da Fundação de Estudos Sociais do Paraná, *e-mail*: <fabiop@fesppr.edu.br>.

1 INTRODUÇÃO

Estudar o Marco Civil da Internet, com vistas às inovações que ocorreram no ciberespaço, na sociedade e no Direito Digital, desperta enorme interesse ao campo jurídico e à sociedade em geral, frente a globalização, efeitos e impactos gerados no ambiente social e no mercado, em âmbito nacional e internacional.

O tema exerce influência sobre o campo do Direito, recaindo nas especialidades ou ramos, uma vez que a Internet transformou as relações socioeconômicas, embora traga inúmeras oportunidades, também riscos que resultam em ônus e bônus aos usuários, provedores e empresas que comercializam produtos e serviços.

Nesse sentido, verifica-se que a tecnologia criou novos modelos de negócio no mundo, praticamente em todos os setores das atividades, que resultaram em interesse jurídico em torno dos prestadores de serviços, produtores de tecnologias, usuários e consumidores, exigindo uma reflexão sobre os princípios constitucionais da livre iniciativa e livre concorrência de mercado, para viabilizar sua continuidade prática. (LIMA, 2016)

A migração dos pontos de venda e do relacionamento com o cliente às plataformas *on-line* e de *e-commerces* tornou imprescindível a análise do contexto histórico, técnico e jurídico, o que permite verificar as ações e os rumos adotados por certos países, em relação às tecnologias, produtos, serviços e seus impactos para a sociedade e para o mercado. (LIMA, 2016)

O Direito Digital representa um dos desdobramentos das inovações recentes, motivado na evolução do Direito como ciência, e introduz um novo pensamento jurídico no campo social diante das características inovadoras e revitalizantes dos processos de gestão e risco.

Os princípios de sustentabilidade aplicados na sociedade digital devem ser garantidos por meio de uma educação pautada em inovação, comprometimento e qualidade da comunicação, transmissão e preservação dos dados e informações transmitidas em tempo real, uma vez que os conteúdos se perpetuam nesse ambiente, gerando danos, do ponto de vista jurídico-social. Deve-se investir no processo de identificação e prevenção de incidentes, valorizando a disseminação de conteúdos autênticos para disponibilizá-los no ambiente virtual, para que contribuam

para formar usuários conscientes e preparados para enfrentar a nova conjuntura disruptiva, sendo o conhecimento um ativo social valioso.

Este estudo apresenta uma análise da regulação do ciberespaço pela legislação brasileira após o surgimento do Marco Civil da Internet e, antes do advento demarcatório, a Lei Carolina Dieckmann e a Lei Azevedo, as quais também regulam crimes dessa natureza. O texto a seguir analisa o ambiente digital e suas consequências quanto a crime/infração penal cometida por menores e adultos, levanta a responsabilidade civil e penal dos pais/responsáveis, aborda a importância da educação escolar tecnológica pautada na ética visando a proteção e segurança dos usuários, levanta os desafios da educação digital, identifica os princípios nos quais se baseiam as Leis 12.735/2012 e a 12.737/2012, ao estabelecerem sanções penais por meio de normas sobre crimes que tenham por objeto sistemas de informações envolvendo dados e informações de terceiros, e, por fim, aponta novos desafios diante de casos recentes de ciberterrorismo e espionagem digital.

2 A REGULAÇÃO DA INTERNET E A PREVISÃO DE DIREITOS E DEVERES PARA O USO DA REDE

Segundo Haikal (2016),

> o uso da Internet criou um ambiente que resultou no aumento de conflitos, uma vez que os *sites* são responsáveis pelos comentários publicados pelos seus leitores. No entanto, deve-se saber de antemão como proceder a retirada de conteúdos disponibilizados no ambiente virtual, especialmente, quando for ofensivo.

Inicialmente, a legislação era genérica, porém, não solucionando situações de origem tecnológica, especialmente, aquelas relacionadas à Internet, gradualmente, certas decisões apontaram soluções frente à insegurança, não somente jurídica, mas também comercial.

O Marco Civil da Internet, introduzido pela Lei nº 12.965/2014, tem natureza peculiar pela sua idealização, criação e discussão, contando com ampla participação dos cidadãos em fóruns de discussão, na Internet e em audiências públicas, promovidas pelo Congresso Nacional Brasileiro.

Haikal (2016) destaca que “um dos temas abordados pela Lei, gerador de debates, é a responsabilidade civil, por divulgar conteúdos em rede.” A Lei envolve diversos deveres aos controladores de sites, que devem remover os conteúdos caso haja denúncia, quando devida, traz o dever de indenizar aos que sofreram danos decorrentes de sua publicação, além da guarda de registros de atividades no ambiente digital de sua propriedade.

A guarda de registros, denominados *logs* de atividades, causam polêmica pelo risco de vigilância aos provedores que oferecem serviços na Internet, diante a ausência de legislação especifica, essa guarda pode ser realizada, por meio de governança interna, com vistas à proteção do direito de terceiros, com prévia ordem judicial para fornecimento. (HAIKAL, 2016)

E caso haja violação quanto ao sigilo dos registros, não se pode afirmar se, de fato, as tecnologias comprovam a má-fé do usuário infrator, sendo o registro coletado e armazenado indispensável para investigar a autoria do ilícito e a veracidade dos crimes cometidos no ambiente virtual, devendo ocorrer a guarda prévia destes, visando promover equilíbrio nas relações e o direito de defesa aos que sofreram abuso por algum tipo criminal ou medida adotada. A ausência de obrigatoriedade na guarda dos dados gera insegurança jurídica e ambiente propício aos que procuram prejudicar a imagem e a reputação de outrem.

O artigo 17 da Lei do Marco Civil da Internet contrapõe-se ao artigo 15, ao eximir os provedores da responsabilidade civil e criminal pela não guarda dos registros de acesso. Em havendo dever legal de armazenagem durante 6 meses, deveria haver o direito de não armazenagem também, questão que deve ser analisada pelo Senado Federal Brasileiro, para receber uma possível emenda. (HAIKAL, 2016)

Outro assunto em destaque é a neutralidade de rede, amplamente discutido nos Estados Unidos (EUA) e na Europa, por envolver o cenário cibernético mundial. Nos EUA a questão gravita em torno da banda larga gratuita ofertada pelo governo americano, porém controlada para evitar o uso não pertinente, como compartilhamento de conteúdo não autorizado e acesso aos serviços ligados a atividades criminosas ou à *deep web.* (ESTADOS UNIDOS, 2017)

Na Europa, questão similar envolve a quantidade de banda usada nos serviços que consomem alto tráfego de dados, como serviços de mensagem

instantânea e *streaming*, similar ao debate que ocorre no cenário brasileiro. (HAIKAL, 2016)

A ideia de neutralidade de rede é inseparável das discussões envolvendo a Internet devido ao acesso sem limite à informação disponível em rede, com exceção de condições exigidas pelo provedor de serviços. No entanto, esse caráter impulsionou a comunicação e o acesso a informações em tempo real e mobilizações nesses últimos anos, como no caso das eleições que ocorreram no Irã, em 2009, a primavera árabe, em 2010, e os protestos brasileiros, em 2013.

O volume de tráfego deve ser solucionado com a implantação de melhorias na infraestrutura e não tolhimento ao acesso a recursos essenciais à população, em diversas regiões e faixas etárias. (WEBER, 2016)

Segundo Haikal (2016), ”existe um procedimento próprio para requisitar dados aos provedores de conexão e acesso, dispensando certos ritos para alcançar tutela.” Os usuários em geral devem conhecer as regras para otimizar o uso de rede e mesmo no sentido de preservar os direitos do usuário sobre recursos inseparáveis do cotidiano da população.

2.1 O MUNDO DIGITAL E SUAS CONSEQUÊNCIAS

Segundo Pinheiro (2016), “o mundo digital é largamente afetado com a promulgação da Lei do Marco Civil da Internet, cuja pretensão é proteger e garantir maior privacidade e maior liberdade ao internauta enquanto usuário dos serviços.” Nesse sentido, o autor afirma que o Marco Civil da Internet tratou do princípio da neutralidade de rede, o qual consiste em garantir igualdade no tráfego de dados, em cujo ambiente todos devem ter acesso igualitário às informações veiculadas e disponibilizadas, seja pelo próprio agente ou por terceiros, sem preferência ao direito.

No entanto, isso não significa que todo internauta que tiver acesso à Internet usufrua de mesma velocidade de navegação, embora seja possível se as operadoras parametrizarem valores aos que desejam conexão rápida; poderá haver preferência na transmissão de determinado conteúdo, em detrimento de outro. Contudo, excepcionalmente, quando o Presidente da República Federativa do Brasil necessite transmitir dados e informações ligadas a soberania nacional, segurança e saúde pública rápida, terá prioridade absoluta, somente nesses casos. (PINHEIRO, 2016)

Conforme Pinheiro (2016),

> o internauta possui seus dados protegidos, desde a aprovação da nova Lei, podendo requerer que sejam apagados, devendo atentar às políticas de privacidade dos serviços, uma vez que o Marco Civil exige a aplicação da Lei nacional envolvendo usuário brasileiro ou que pelo menos uma das partes esteja no Brasil, mesmo que o provedor de serviços esteja em país diverso.

O Marco Civil está relacionado com o uso responsável do princípio de liberdade de expressão, embora não seja fácil remover conteúdo ofensivo de forma rápida, exceto, envolvendo imagens de nudez, cenas sexuais e exposição de crianças e jovens menores de 18 anos no ambiente virtual, aplicável o Estatuto da Criança e do Adolescente (ECA). Nesses casos, a denúncia pode ser feita online, na plataforma, devendo o conteúdo ser imediatamente removido do ar. Para outras ocorrências, as publicações serão removidas via requerimento encaminhado ao Juiz que, uma vez autorizado, por ordem judicial serão removidos.

Segundo Farah (2016),

> conteúdos disponibilizados na Internet são rastreáveis e a captura de telas dos equipamentos tecnológicos, como computadores, celulares e *tablets* devem ser feitas com o fito de comprovar o crime e sirvam de testemunha sobre os conteúdos abusivos publicados.”

Deve-se registrar por meio de ata notarial ou através de telas gravadas. Porém, a guarda de evidências eletrônicas (logs) configura o registro dos fatos no ambiente virtual, associado a autoria (*login*) de quem postou os arquivos online, torna-se relevante; ao passo que somente vestígios de fatos, mas sem prova, não configuram a autoria do crime. (FARAH, 2016)

Os provedores de conexão e aplicação armazenam dados em ambientes de navegação, devendo preservar seus registros durante um ano, no caso do primeiro, e de seis meses, no segundo caso, e seus responsáveis devem atender o mandado judicial, somente nessa hipótese. (PINHEIRO, 2016)

O internauta deve adotar certos cuidados quanto ao uso e disposição de conteúdos lançados no ambiente virtual, seja em sua forma escrita ou em imagens lançadas, pela impossibilidade de que permaneçam no anonimato e pela capacidade própria em removê-los.

O mundo digital existe para todos, devendo o internauta repensar na publicação e compartilhamento dos conteúdos considerados abusivos. Na atualidade, vive-se na era digital, um mundo que exige transparência e pela impossibilidade de escondê-los, pois além dessas informações se espalharem muito rapidamente, existem inúmeros meios para rastreá-los, sem anonimato. O Marco Civil da Internet representa um passo importante na proteção de valores na era digital, embora, ainda haja muito o quê fazer nesse campo. (PINHEIRO, 2016)

2.2 RESPONSABILIDADE CIVIL DOS PAIS E RESPONSÁVEIS

Segundo Lima (2016), pais e responsáveis devem se atentar para a conduta de seus filhos, uma vez que no ambiente virtual poderá haver quem pratica atitudes desautorizadas pela Lei. Mas para que haja um sujeito ofendido, é necessário que a ofensa seja provada; contudo, tanto pode-se ofender, quanto ser ofendido decorrente da má conduta do internauta, resultando em dano e consequente indenização.

De acordo com o teor publicado, poderá desencadear ônus financeiro, resultar na contratação de advogado e na participação do infrator em audiências na presença do juiz, uma vez que em ofensas realizadas via Internet a legislação prevê a incursão em crimes de injúria, difamação e calúnia, mas as penas atribuídas configuram pequenas sanções, pois quando praticadas dificilmente recebem condenação com liberdade tolhida. (LIMA, 2016)

Certamente será um transtorno no caso de menores, devendo seus pais e responsáveis comparecer à delegacia especializada de crianças e adolescentes. O Poder Judiciário deve se atentar quanto à abrangência do dano utilizando-se de indenizações para inibir a conduta ilícita, uma vez que o Estatuto da Criança e do Adolescente estabelece sanções com repercussão na família e na sociedade, aos infratores. (LIMA, 2016)

2.3 EDUCAÇÃO EM ÉTICA E SEGURANÇA

Nessas últimas décadas, com destaque especial aos últimos quinze anos, as instituições de ensino passaram por profunda transformação, não somente na sala de aula, mas em todas as relações com a comunidade escolar. A Internet e as novas ferramentas de ensino-aprendizagem são responsáveis por mudanças significativas,

mas parcela relevante dessa revolução no ensino está ocorrendo dentro dos lares, no ambiente familiar. (PINHEIRO, 2016)

O fornecimento de tecnologias às crianças e aos jovens indiscriminadamente na era digital a família passa exercer papel ativo e assume os riscos arcando com o ônus na esfera civil e penal frente a prática do ilícito.

É possível educar construindo modelos, participando com comprometimento e acompanhamento dos responsáveis; o exemplo começa no lar, envolve a redefinição de papéis uma vez que as instituições de ensino não têm controle ao acesso do conhecimento (tecnologias), nem mesmo os pais, muitas vezes. Verifica-se que o ensino presencial gradualmente está sendo substituído pela educação a distância (EaD), sem contato e interação na relação professor-aluno.

O aluno deve ser orientando a aperfeiçoar-se e desenvolver-se, com respeito mútuo, usufruindo da liberdade com responsabilidade, princípio norteador da relação professor-aluno, não importando a época nem qual tecnologia utiliza-se a serviço do ensino-aprendizagem, uma vez que poderá ser prejudicar nos resultados finais.

Segundo Pinheiro (2016),

> não somente a Instituição de Ensino, mas também os pais, têm o solene dever de educar e corrigir seu filho-aluno (crianças e jovens) acerca do uso seguro, sustentável, ético e legal de ferramentas tecnológicas, no lar, em sala de aula ou no ambiente social, para que deem destinação adequada ao uso e fruição de seus aparelhos tecnológicos ou da escola, bem como o acesso coerente à Internet.

O que se questiona é como formar pessoas digitalmente corretas, para que identifiquem limites morais e éticos quanto ao uso da tecnologia, devendo envolver regras claras e incorporar princípios para formar indivíduos mais conscientes na era digital. A solução para reduzir esses incidentes em ambientes educacionais depende do uso da própria informação para prevenir e direcionar condutas visando criar o senso coletivo em questões digitais. (PINHEIRO, 2016)

E um momento transitório, em que as leis não atendem casos novos que surgem no ambiente digital, é dever do Poder Judiciário legislar sobre situações que se transformam em ações judiciais. Portanto, é fundamental que a Instituição de Ensino organize e lidere campanhas sobre conscientização coletiva dos jovens e adultos para o uso consciente dos novos recursos digitais.

E embora pareça não haver relação direta com a prestação dos serviços de ensino, incidentes envolvendo o *WhatsApp* e outras mídias sociais, caberá à educação não permanecer silente ou compactuar com condutas inadequadas, independente de quem sejam os responsáveis, uma vez que tais condutas afetam o ambiente educacional, embora indiretamente.

Segundo Pinheiro (2016),

> “e mesmo diante de tais orientações descumprir o combinado deve-se aplicar medidas socioeducativas, requerendo, caso necessário, medidas administrativas em âmbito educacional ou judicial, visto que a omissão ou negligência poderá atrair responsabilidade solidária da Instituição de Ensino em eventual dano causado à outrem, vinculado às relações desta com os integrantes da comunidade escolar.

2.4 DESAFIOS DA EDUCAÇÃO NO MUNDO DIGITAL

A sociedade digital transformou definitivamente o modo pelo qual as pessoas se relacionam na sociedade, uma vez que toda pessoa tem poder para expressar-se em tempo real no mundo digital, não importando raça, situação econômica, função, cargo e hierarquia de valores culturais, gerando conteúdos que se perpetuam no ambiente da Internet. No entanto, o que era para ser positivo, usado sem critérios, pode tornar-se negativo, envolvendo desde ofensas no ambiente digital ao plágio até de outros crimes que podem ser praticados nesse mesmo ambiente. (PINHEIRO, 2016)

Segundo Pinheiro e Haikal (2016),

> jovens nascidos e criados com o rigor de aparatos tecnológicos, impulsionados pela insegurança que existe no mundo real, passam a viver uma vida mais virtual que real, inspirados em eventos visualizados na Internet, com amigos e interações fundamentadas nas redes sociais, devendo ser monitorados e cuidados por seus pais e responsáveis.

Não apenas por se tornarem vítimas algozes, mas por não estarem ainda em desenvolvimento e não se tornarem infratores.

Os professores devem tornar-se educadores mais presentes e interativos nas relações com seus alunos, sempre conectados, utilizando-se da nova linguagem *web*, com a missão de demonstrar a existência de princípios, regras, limites, uso e fruição saudável e segura da tecnologia, com fins particulares, mas também sociais.

A Internet traz a rua para dentro do lar das famílias brasileiras e os costumes do lar e das ruas para dentro da escola. No entanto, muitos de seus pais trabalham

diariamente no computador, ao chegarem à noite, procuram distanciar-se da tecnologia e acabam não se inteirando na rotina da vida digital de seus filhos, delegando ao Google ou à Wikipédia a importante tarefa. (PINHEIRO, 2016)

O fato é que devem refletir sobre o fato, uma vez que os principais riscos digitais assemelham-se ao mundo real, seja falar com pessoas desconhecidas, sofrer assédio, acesso aos conteúdos inapropriados à idade, exposição de sua intimidade e tornar-se vítima de ofensa. Ao liberar celulares adaptados com câmera aos filhos, devem ensinar-lhes acerca dos riscos de obter a imagem de outras pessoas sem a devida autorização, quanto mais publicá-las na Internet. (PINHEIRO, 2016)

Nesse sentido, o jovem deve estar orientado quanto ao uso da tecnologia e, conforme a confiança e responsabilidade conquistada, passar a ganhar autonomia, sendo esse um papel da escola e da família.

E diante do uso excessivo, cresceu significativamente o número de incidentes envolvendo crianças e jovens no uso da Internet, inclusive, dentro da escola, principalmente, devido à má educação no campo digital. E pior, devido a isso, certos usuários utilizam-se do conhecimento em tecnologias de ponta para produzir o ilícito para outras pessoas, sejam colega de escola, professores ou desconhecidos. (PINHEIRO e HAIKAL, 2016)

A escola, os pais e os professores são responsáveis pela orientação ao aluno sobre a boa conduta digital, começando pelo uso adequado de seus dispositivos, e por mostrar e advertir sobre os termos de uso da tecnologia e de redes sociais como Facebook, Twitter, entre outros.

Nesse sentido, nota-se que os professores devem apropriar-se dos saberes presentes em manuais específicos, que versam sobre o uso da tecnologia e sobre as normas de uso e fruição da rede, para conscientizar jovens e crianças, pois a um único click irrefletido poderão envolver-se em sérios riscos, estando dentro do lar ou da escola. E quando não, certos jovens se fazem passar por maior idade para serem inseridos mais facilmente no ambiente digital, em que a idade mínima permitida é aos 13 anos, porém, desconhecedores de normas específicas infringem conceitos éticos básicos e a própria lei, atirando-se na esfera penal. (PINHEIRO e HAIKAL, 2016)

A escola não deve somente investir em infraestrutura tecnológica, com a instalação de portais educacionais, EaD, wireless, *tablets*, lousa virtual e outras

tecnologias de apoio à educação, diante do perigo das ferramentas, sem uma adequada orientação. Mais que tecnologias disponíveis em sala de aula, deve-se ensinar regras de uso, sobre as leis vigentes, importância da ética na era digital, uma vez que a liberdade de expressão exige responsabilidade. (PINHEIRO, 2016)

2.5 LEIS DE CRIMES DIGITAIS

Segundo Pinheiro e Haikal (2016), a Lei n. 12.735/2012 (Carolina Dieckmann) e Lei n. 12.737/2012 (Azeredo) autorizam a aplicação penal de normas específicas sobre crimes digitais próprios, configurados, que tenham como objeto dados, informações e sistemas de informação, em contraponto aos crimes digitais impróprios em que os sistemas de informação servem como fonte à prática do delito.

Nesse sentido, conforme os autores, desde a promulgação dessas leis recentes, o usuário também é responsável pela proteção de seus dispositivos, diante da responsabilização atribuída aos invasores de dispositivos alheios para obtenção ilícita de dados e informações.

As sanções aplicadas vão desde a pena de detenção, que varia de três meses a dois anos de reclusão, com o agravante de aumento segundo o prejuízo econômico causado, divulgação e vazamento de dados na Internet, conteúdos obtidos ligados às comunicações eletrônicas privadas, segredo comercial e industrial, informação sigilosa e invasão por controle remoto não autorizado ao dispositivo. (PINHEIRO e HAIKAL, 2016)

A Lei n. 12.737/2012 (Carolina Dieckmann), à luz do Código Penal Brasileiro (1988), em seu art. 266, estabeleceu o tipo penal de invasão aos sistemas de informação ilegítima, ampliando o crime de indisponibilização dos serviços públicos, equiparando o cartão magnético ao documento particular para que a falsificação de cartões de débito/crédito se torne punível, porém, o tipo penal exige requisitos para configurar crime.

O praticante desse tipo de delito recebe sanções similares àquele que instala vulnerabilidade em um sistema de informação para obter vantagem indevida, como um *backdoor* ou realize determinada configuração para que portas de comunicação à Internet estejam sempre abertas (PINHEIRO e HAIKAL, 2016).

O usuário de *gadgets* e dispositivos informáticos comuns está protegido de *hackers* e pessoas mal intencionadas que abusam da confiança e intencionalmente procuram devassar dispositivos para prejudicar seu proprietário, pela exclusão ou

alteração de dados, para se tornarem imprestáveis ou apropriar-se de dados do computador com informações íntimas e privadas (fotos, documentos e vídeos).

No Brasil, as empresas passam a usufruir de maior proteção jurídica contra espionagem digital, de forma que a obtenção de segredos comerciais e informações sigilosas foram, além definidas, também tratadas em termos de sanções a serem aplicadas. (PINHEIRO e HAIKAL, 2016)

A Lei n. 12.735/2012 (Azeredo) incorporou duas disposições jurídicas relevantes: a primeira indica que a polícia judiciária, mediante regulamentação e autoridade, deve preparar-se para combater severamente os crimes digitais; no caso de crime de discriminação, fixados pela Lei n. 7.716/1989, o juiz pode determinar a retirada de conteúdo discriminatório veiculado em estações de rádio, canais de TV e Internet e quaisquer outros meios. (PINHEIRO e HAIKAL, 2016)

No entanto, as penas parecem relativamente pequenas, ao enquadrar o crime como sendo de menor potencial ofensivo, não coadunando com a proteção dos ativos intangíveis, que são a pedra angular da sociedade da informação. A apropriação indevida de dados pode resultar prejuízo de larga escala, incomparável ao furto comum; portanto, não deveria receber pena menor, sobretudo, em caso de espionagem, que pode conduzir à concorrência desleal.

Tais leis não esgotaram os tipos penais digitais, o que remete ao fato de ser impossível desconsiderar crime a indisponibilidade dos sistemas de informação de empresas privadas, como sites de comércio eletrônico, bancos, disseminação de vírus e códigos maliciosos em razão da interconexão com a sociedade atual. (PINHEIRO e HAIKAL, 2016)

No entanto, o legislador se descuidou ao não indicar que a invasão de dados requer a presença do fator obtenção, modificação e exclusão de dados, visto que bisbilhotagem e envio de dados para terceiros podem desviar o tipo penal e a invasão de dispositivos sem mecanismos de segurança desconfigura a prática de crime. (PINHEIRO e HAIKAL, 2016)

Nesse sentido, a não obrigatoriedade na guarda de logs de conexão e acesso pode inviabilizar a instrução criminal devido à dificuldade na identificação do agente. E para maior proveito da Lei. a proteção dos dispositivos particulares é indispensável. (PINHEIRO e HAIKAL, 2016)

Dessa forma, veja-se a seguir alguns mecanismos de proteção aos dispositivos particulares ou empresariais (PINHEIRO e HAIKAL, 2016):

a) Utilizar proteção sempre com senha, código e dados biométricos com o fito de impedir acesso desautorizado, valendo para computadores de mesa, *notebooks*, *tablets*, *smartphones*, reprodutores portáteis de áudio/vídeo;

b) Deixar sistemas de *firewall* e detecção de intrusão sempre ativo, com perfil de atividades maliciosas atualizado e refinado para evitar o falso-positivo;

c) Quando o usuário perceber atividade suspeita, comunicar a autoridade policial, buscando imediatamente a ajuda de especialistas, e evitar usar o dispositivo para que as provas digitais sejam preservadas em caso de perícia.

2.6 CIBERTERRORISMO E GUERRA CIBERNÉTICA

Segundo Pinheiro (2016), os atentados ocorridos em Paris, em 2015, levantaram acalorados debates internacionais, visando combater o terrorismo desde as bases digitais, uma vez que o campo da Internet tornou-se alvo para atrair jovens de todas as idades e classes, para atuar em propostas radicais extremadas.

A reação aos tais eventos somente ocorre após a fatalidade ser consolidada, exigindo que as autoridades invistam na prevenção e detecção de crimes dessa natureza, pois tais ações geralmente são arquitetadas com muita antecedência, envolvendo pessoas que se conectam e interagem no campo digital. O que remete afirmar que a batalha contra o terrorismo representa uma nova fronteira, mais conhecida como o território *deep web*.

Pinheiro (2016) afirma que inúmeras práticas ilícitas se disseminaram ao redor do mundo e concentram-se na *deep web*, incluindo crime de pedofilia, tráfico de drogas, terrorismo, armas e materiais controlados. Na atualidade, as bitcoins, moeda que circula somente em ambiente virtual, contribui para lavar dinheiro digital, dificultando rastrear a origem e destino dos recursos.

Nessa esfera, nota-se que o ambiente do terror não é somente físico, sem um local específico, recruta indivíduos dos diversos extremos do planeta e atinge dimensão planetária, cujos integrantes são treinados remotamente, por meio de recursos tecnológicos, similar ao ensino EaD, de reuniões via *WhatsApp* ou *Skype* em grupo.

A tecnologia propriamente dita não traz consigo um mal intrínseco, tudo depende de como é utilizada pelos usuários. Para isso, deve-se criar princípios que visem promover a segurança pública e a defesa digital, estrategicamente, planejar

campanhas de alerta ao cidadão, que está na linha de frente no combate ao terror, maior vítima de ataques. (PINHEIRO, 2016)

Araújo (2017) questiona:

> o modo pelo qual os operadores da Internet poderão contribuir para combater o ciberterrorismo de forma efetiva? Como as autoridades podem derrubar sites que promovem a intolerância cultural, religiosa, política e o terror no mundo digital e físico?

Segundo Amaral (2008),

> ciberterrorismo vem ser toda a atividade praticada pela Internet ou via dispositivos digitais, que visam causar pânico e sensação de insegurança, desde propagação de boatos com evidências falsas de ataque maciço de negação aos serviços e alteração de dados.

Isso torna o sistema de um país ou mundial crítico, ao afetar os campos de distribuição de energia, saneamento básico, controle e fluxo de água e trânsito, entre outros problemas que se configurem. Verifica-se a existência de uma linha tênue que separa o direito à manifestação pacífica da opinião praticada pelo *hacktivismo* do bem versus manifestações com propostas terroristas.

Muitas vezes, os ataques são direcionados às empresas, para determinada marca ícone que integra uma cultura ou similar ao ocorrido em 2015 (janeiro), em Paris, em que as pessoas, cujo ofício era criticar, de forma satírica e jocosa, ou ainda o fanatismo religioso que assola o mundo, resultando em um grande número de mortes.

Após os ataques sofridos pela redação da Revista Charlie Hebdo, o grupo Anonymous publicou um vídeo deflagrando a *#OpCharlieHebdo*, em que seus esforços foram direcionados ao combate do terrorismo islâmico e aos responsáveis pelo episódio terrorista na capital francesa.

No sentido de pensar sobre tais fatos, será que se estaria ingressando na Terceira Guerra Mundial, por meio da guerra digital? Pelo que parece, já está acontecendo nos bastidores da Internet, embora em uma escalada pequena e silenciosa. (PINHEIRO, 2016)

Um caso notável de invasão ao ciberespaço foi em 2014, quando a divisão de entretenimento da empresa Sony sofreu ataques cibernéticos, dirigidos à Coreia do Norte, ensejando resposta dos Estados Unidos, deixando o país asiático

desconectado por aproximadamente 24 horas; mas não foi a primeira vez. Em 2009, cerca de 25 *sites* da Coreia do Sul foram invadidos, quando o *malware*, conhecido como Careto (*the mask*), promoveu ataques em mais de 10 países, desde 2007.

Em 2007, outro caso interessante envolvendo a Rússia contra a Estônia, quando as instituições financeiras, os sistemas de telecomunicações e sites de notícias desse país foram completamente bombardeados por ataques de denegação aos serviços públicos e privados. (PINHEIRO, 2016)

Pinheiro (2016) considera:

> o ciberespaço vulnerável, pois grande parte das autoridades públicas e líderes empresariais não tratam da segurança digital como prioridade absoluta na pauta de estratégias de seus país. No entanto, esse amadorismo, por um lado e grupos armados e profissionais, de outro, estão se organizando a cada dia.

Por isso, deveria haver uma agenda comum, com compromissos de ação conjunta entre a iniciativa público-privada, abrangendo países diversos, com o fito de garantir maior disponibilidade de recursos e serviços essenciais de combate ao ciberterrorismo, sobretudo, preparando a população para um cenário bélico para atuar na guerra digital. (PINHEIRO, 2016)

2.7 LEGALIDADE DA ESPIONAGEM DIGITAL

Segundo Pinheiro (2016),

> obter conhecimento sobre informações sigilosas de maneira privilegiada remete-se ao conceito de espionagem, frente o interesse entre a informação obtida e o valor agregado ao que interessa favorecer-se com a mesma, por representar fonte de conhecimento e privilégio.

Na atualidade, a espionagem tem sido um conceito acompanhada do vazamento de informações e pretende revelar, para terceiro não autorizado, informação considerada sigilosa, porém, obtida de forma ilegítima ou clandestina, sem que seu proprietário tenha ciência ou devidamente autorizado sua coleta e compartilhamento da mesma com outros ou que o torne pública. (PINHEIRO, 2016)

No entanto, a espionagem resulta em danos aos que sofrem ataque; mas casos excepcionais não configuram espionagem. Contudo, no ciberespaço nem sempre é fácil saber a verdade dos fatos. E, segundo os manuais militares, o termo

espionar remete-se diretamente aos serviços de inteligência, que visam obter determinada informação. (PINHEIRO, 2016).

A proteção contra a espionagem envolve o manejo de serviços de contrainteligência para assegurar a preservação e integridade dos dados e informações. Diante do exposto, fica evidente que o mundo está integrado a sociedade do conhecimento, o que leva conceber que quase todo tempo alguém está espionando ou sendo espionado. (PINHEIRO, 2016)

E, assim sendo, se espionagem configura uma técnica, o *modus operandi* do sujeito, que dispõe a cada dia mais de ferramentas tecnológicas para executar o ilícito, representa poder, determinando o domínio político e econômico de uma instituição sobre as outras, em caso de espionagem industrial e comercial, ou de um país sobre outro, resultando em uma espécie de guerra dos dados ou guerra digital. (PINHEIRO, 2016)

Segundo o Relatório do Federal Bureau of Investigation (FBI) - (2017), quanto mais conectadas as pessoas se encontrarem, maior a possibilidade de serem espionadas eletronicamente, facilitado pela falta de hábito de segurança digital em nível endêmico-cultural. (PINHEIRO, 2016)

E quando, afinal, um ato de espionagem entre países diversos seria legítimo? Existem formas de tornar a espionagem legal? Essa resposta pode remeter-se aos casos envolvendo países como Alemanha, China, Estônia, Nova Zelândia, Austrália, Índia, Irã, Iraque e Rússia. E como ficaria a legislação em torno do assunto, não somente de cada país individualmente, mas em âmbito global?

Veja-se o efeito 9/11, que gerou o Patriot Act, nos EUA, em que a seção 215 forneceu poder jurídico à autoridade americana usar qualquer meio que permitisse acesso ilimitado a uma informação que venha contribuir para promover proteção e segurança nacional no país. Ou seja, abriu as portas para visualizar todo e qualquer tráfego de dados que se torne relevante em investigações de combater a ameaças à segurança nacional, traduzido, remete-se ao combate ao terrorismo.

E para os demais países, sejam aliados ou não, o Congresso Norte-Americano, representado pelo legislativo, deu carta branca ao afirmar que praticamente tudo quanto for contra os EUA passa ser considerado terrorismo. No Brasil, porém, não há nada que se equipare ou assemelhe à medida adotada. (PINHEIRO, 2016)

Em qualquer momento da história humana sempre houve e continua havendo riscos no uso de estratagemas como flagrante preparado, interceptação e tortura, no intuito de fornecer segurança à coletividade, se as investigações não seguirem o devido processo legal, visando a não arbitrariedade da autoridade e o abuso de poder.

No âmbito privado, as leis modernas protegem as empresas contra a espionagem, com previsão legal contra crimes diversos, como revelação de segredo, à luz do Código Penal Brasileiro, art. 154. No entanto, a Lei n. 12.737/2012 (Carolina Dieckmann), no artigo 154-A, evidencia o uso de informações não autorizadas de celebridades (entes privados), ao crime de interceptação previsto na Lei n. 9.296/1996. (PINHEIRO, 2016)

Em âmbito público, mais especialmente entre países, há carência de definição e existência de regras claras em como ocorre o jogo político internacional, global e sem fronteiras claras. Na atualidade, não se espiona mais o inimigo, espiona-se qualquer indivíduo ou empresa privada e pública, em qualquer lugar, a qualquer momento; basta haver interesse ou, com poder do *big data*, basta haver o poder de processamento.

No varrer das páginas da Internet e suas redes sociais, podem ser descobertos segredos industriais que em outras épocas eram guardados durante anos. Em muitos casos, nem sequer configura ato de espionagem, presumindo que esse incidente somente ocorre quando a informação for protegida; de igual forma, verifica-se que não há crime em caso de invasão se a porta estiver aberta. E quando as pessoas publicam algo (qualquer coisa), seja sua rotina diária, horários, trajetos, projetos, trabalho e mesmo conteúdos sobre outras pessoas, basta alguém olhar e descobrir as informações publicadas. (PINHEIRO, 2016)

Por fim, nota-se que, desde a navegação no *Facebook* ao uso de *sniffer* para busca de dados em máquinas alheias, banalizou-se não somente a espionagem, mas também o acesso à informação privilegiada. No entanto, o melhor método para combater a espionagem ainda é a educação pautada na segurança da informação. Além disso, é essencial que tratados internacionais sejam celebrados entre países, especialmente, na arena política, econômica e de mercado mundial para que sejam definidas novas regras para esse campo.

3 CONSIDERAÇÕES FINAIS

Ressalta-se, por fim, que cabe ao Direito adaptar-se ao tratamento dos conflitos nos ambientes virtuais. No Brasil, o Direito Digital respalda-se na recente aprovação do Marco Civil da Internet e na legislação que surgiu na segunda década do século XXI, visando promover maior segurança no ciberespaço, diante dos impactos sociais e jurídicos vivenciados em uma era genuinamente digital. As transformações sociais exigem que o Direito e seus ramos especialistas se atualizem constantemente, para atender as requisições sociais e jurídicas. Diante das mudanças de comportamento e o modelo socioeconômico vigente, o Direito Digital tem recebido aportes teóricos significativos desde o início da década de 90, época em que surgem as primeiras obras sobre o tema no Brasil, sendo a maioria de berço acadêmico, relacionando o Direito às novas tecnologias.

Ao que tudo indica, em um mundo progressivamente digital, em que o ambiente virtual passou a ser uma extensão da vida real, por meio de relações de consumo, transações bancárias, troca de informações e convívio social, o debate do Direito Digital segue no sentido de acompanhar as transformações do meio.

REFERÊNCIAS

AMARAL, S. A. do. Gestão da informação e do conhecimento nas organizações e a orientação de marketing. **Informação & Informação**. Londrina, 2008;13 (seção especial):52-70.

ARAÚJO, C. C. **Diferença entre ciberterrorismo e ciberativismo.** (2017). Disponível em :<http://exploit.araujo.cc/blog/o-que-e-hacktivismo-qual-a-diferenca-entre-cyberterrorismo-ou-cyberativismo.html>. Acesso em: 10 de out. 2017.

ESTADOS UNIDOS. Federal Bureau of Investigation. **FBI** (2017). Disponível em: <www.ic3.gov>. Acesso em: 5 mar 2018.

FARAH, Rafael Mott. A responsabilidade dos estabelecimentos comerciais no fornecimento de rede wi-fi a seus clientes. In: PINHEIRO, Patrícia Peck (coord.). **Direito digital aplicado 2.0**. 2.ed. São Paulo: Thomson Reuters, 2016.

HAIKAL, Victor Auilio. Enfim, o marco civil da internet. In: PINHEIRO, Patrícia Peck (coord.). **Direito digital aplicado 2.0**. 2.ed. São Paulo: Thomson Reuters, 2016.

_____. Da necessidade de inclusão de URL em ordens judiciais. In: PINHEIRO, Patrícia Peck (coord.). **Direito digital aplicado 2.0**. 2.ed. São Paulo: Thomson Reuters, 2016.

LIMA, Glaydson de Farias. **Da responsabilidade jurídica dos pais e responsáveis**. Manual de direito digital: fundamentos, legislação e jurisprudência. Curitiba: Appris, 2016.

_____. **Manual de direito digital**: fundamentos, legislação e jurisprudência. Curitiba, Appris, 2016.

PINHEIRO, Patrícia Peck; HAIKAL, Victor. Nova lei de crimes digitais. In: PINHEIRO, Patrícia Peck (coord.). **Direito digital aplicado 2.0**. 2.ed. São Paulo: Thomson Reuters, 2016.

PINHEIRO, Patrícia Peck. Guerra digital e ciberterrorismo. In: PINHEIRO, Patrícia Peck (coord.). **Direito digital aplicado 2.0**. 2.ed. São Paulo: Thomson Reuters, 2016.

_____. Educação em ética e segurança. In: PINHEIRO, Patrícia Peck (coord.). **Direito digital aplicado 2.0**. 2.ed. São Paulo: Thomson Reuters, 2016.

_____. Como educar os jovens na era digital. In: PINHEIRO, Patrícia Peck (coord.). **Direito digital aplicado 2.0**. 2.ed. São Paulo: Thomson Reuters, 2016.

PINHEIRO, Patrícia Peck. Espionagem digital e legal. In: PINHEIRO, Patrícia Peck (coord.). **Direito digital aplicado 2.0**. 2.ed. São Paulo: Thomson Reuters, 2016.

SANTOS, Coriolano Aurélio de Almeida Camargo. Prefácio. In: PINHEIRO, Patrícia Peck. (coord.). **Direito digital aplicado 2.0**. 2.ed. São Paulo: Thomson Reuters, 2016.

WEBER, Sandra Paula Tomaz. A utilização da assinatura eletrônica biométrica na formação dos contratos. In: PINHEIRO, Patrícia Peck (coord.). **Direito digital aplicado 2.0**. 2.ed. São Paulo: Thomson Reuters, 2016.

GLOSSÁRIO

Backdoor: recurso utilizado por diversos *malwares* para garantir acesso remoto ao sistema ou à rede infectada, explorando falhas críticas não documentadas existentes em programas instalados, *softwares* desatualizados e do *firewall* para abrir portas do roteador.

Big Data: conceito desenvolvido para unir e interpretar informações, prevendo tendências e ajudando na tomada de decisões estratégicas.

Bitcoins: moeda virtual que permite aos usuários conduzir transações no anonimato, extensamente utilizada na 'internet invisível' para o comércio de produtos e serviços de variados tipos.

Código Malicioso: é um termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador.

Deep Web: designação para determinada zona da internet que não pode ser facilmente detectada pelos tradicionais motores de busca, garantindo privacidade e anonimato aos navegantes, formada pelo conjunto de sites, fóruns e comunidades que costumam debater temas de caráter ilegal e imoral.

Firewall: dispositivo de rede de computadores que tem por objetivo aplicar políticas de segurança para determinado ponto da rede.

Gadgets: comumente chamados de *gadgets* dispositivos eletrônicos portáteis como PDAs, celulares, smartphones, leitores de MP3, entre outros.

Hackers: designa programadores maliciosos e ciberpiratas que agem com o intuito de violar ilegal ou imoralmente sistemas cibernéticos.

Hacktivismo: junção da palavra hacker e ativismo, uma forma de protesto contra governos e empresas, promovendo ideias em relação à liberdade política e de expressão, direitos humanos, ética, entre outras.

Log: expressão usada para descrever o processo de registro de eventos relevantes em um sistema computacional.

Malware: programa de computador destinado a infiltrar-se em sistemas de computador alheio de forma ilícita, no intuito de causar danos, alterando ou roubando informações (confidenciais ou não).

Roteador: dispositivo que encaminha pacote de dados entre redes de computadores.

Sniffer: ferramentas que interceptam e analisam o tráfego de uma rede, com ele você pode descobrir quais sites estão sendo acessados na rede.

Vírus: *software* malicioso que é desenvolvido por programadores geralmente inescrupulosos. Tal como um vírus biológico, o programa infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática.