Revista Eletrônica ***Pesquiseduca***
Revista do Programa de Educação - Universidade Católica de Santos
ISSN: 2177-1626

A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD

Consumer (hiper)vulnerability in cyberspace and the LGPD perspectives

Lucas de Souza Lehfeld[1]
Alexandre Celiot[2]
Oniye Nashara Siqueira[3]
Renato Britto Barufi[4]

Resumo: O trabalho investiga a extensão da vulnerabilidade do consumidor no ambiente do ciberespaço. O objetivo da pesquisa é analisar o contexto evolutivo informacional que culminou na Era da Informação para delinear como esta nova realidade impulsionou o âmbito consumerista, mormente no que tange ao acesso do comércio de dados pessoais e à ocorrência de crimes pelas vias digitais que são, cada vez mais fáceis, comuns e de difícil solução. Visa-se estabelecer um paralelo entre o avanço da tecnologia com a ocorrência dos cibercrimes para então verificar a extensão da aplicabilidade e eficácia da nova Lei Geral de Proteção de Dados (LGPD) na proteção do consumidor frente a práticas abusivas das empresas e condutas delituosas de criminosos digitais. A pesquisa foi realizada através de revisão bibliográfica, de caráter exploratório na doutrina, jurisprudência e dados estatísticos, discorrendo em paralelo sobre a preocupação com a proteção de direitos fundamentais.

Palavras-chave: Vulnerabilidade. Consumidor. Crimes cibernéticos. LGPD.

Abstract: The paper investigates the extent of consumer vulnerability in cyberspace. The objective of the research is to analyze the evolutionary informational context that culminated in the Information Age in order to outline how this new reality has boosted consumerism, especially with regard to the accession of personal data trade and the occurrence of crimes through digital channels, which are increasingly easier, more common and more difficult to solve. It aims to establish a parallel between the advancement of technology and the occurrence of cybercrimes, and then verify to what extent the new General Data Protection Law (LGPD) is applicable and efficacious in consumer protection against abusive practices by companies and digital criminals' conduct. The research is based on literature review, is exploratory in doctrine, jurisprudence and statistical data, and in parallel approaches the concern with the protection of fundamental rights.

Keywords: Vulnerability. Consumer. Cyber crimes. LGPD.

[1] Doutor em Direito pela Pontifícia Universidade Católica de São Paulo.
[2] Mestrando pela Universidade de Ribeirão Preto – UNAERP. Bolsista PROSUP/CAPES.
[3] Mestranda pela Universidade de Ribeirão Preto – UNAERP. Bolsista PROSUP/CAPES.
[4] Mestrando pela Universidade de Ribeirão Preto – UNAERP

Introdução

Com o advento da Internet a partir de 1960 e sua maior difusão em 1990, houve profunda alteração no modo com que as pessoas enxergavam o mundo e relacionavam-se umas com as outras. O conceito de distância e informação foi se transformando, de tal forma que a distância física deixou de representar um obstáculo real às relações sociais e transações em geral. No mesmo sentido, a velocidade no fluxo de acesso e disseminação das informações torna-se o paradigma do final do século XIX, facilitando, em uma estrutura aberta, globalizada e interligada, a formação de banco de dados com possibilidades infinitas de armazenamento de informações dos usuários da internet.

O espaço online ou cibernético é tido como um novo ambiente social, paralelo e permanentemente vinculado ao real, que traz desafios sobre suas implicações e consequências nas relações humanas na denominada Era da Informação, isso é, o fácil acesso aos cidadãos trouxe benefícios e consequências. No mesmo sentido, as transformações tecnológicas têm sido tão profundas que não se limitam somente à utilização particular da internet. Empresas por todo o mundo dependem da conectividade para concretizarem suas ofertas, vendas, comunicações, armazenamento de informações e demais operações no ambiente dos negócios. Na medida em que tem se tornado comum a utilização desses dados por empresas privadas e entidades governamentais, os quais muitas vezes são armazenados e obtidos sem o conhecimento e/ou consentimento consciente do usuário, revela-se importante discutir os limites e implicações da privacidade no meio cibernético.

As informações inseridas de forma incontrolável no mundo digital proporcionaram, indiscutivelmente, avanços e melhorias nas relações interpessoais e modo de vida das pessoas. Outrossim, todas as facilidades trazidas e criadas graças à expansão da conectividade se afiguram difíceis de serem acompanhadas por meios de efetiva proteção aos seus usuários, o que vulnerabiliza, ainda mais, a situação do consumidor quando atua no ciberespaço. Aqueles com elevado conhecimento tecnológico têm-se aproveitado dessas situações para obter vantagens ilícitas pela prática dos chamados crimes cibernéticos.

Queremos dizer, assim, que a internet não é um lugar totalmente seguro, o que, pela via obliqua, acaba por violar direitos fundamentais. Ou seja, em razão da incomensurável expansão do ciberespaço e da falta de proteção e conhecimento técnico do consumidor, esse acaba tendo sua vida, honra, intimidade e privacidade ao

alcance de um clique de pessoas mal intencionadas que se aproveitam do anonimato e/ou ausência de punição para praticar violar direitos. Dados apontam que, a nível global, 65% dos adultos já foram vítimas de algum tipo de crime digital. No Brasil, esse número chega a 76% dos adultos, sendo a China a maior vítima, com 83% da população adulta vítima desse tipo de crime (NORTON, 2018). O número expressivo de crimes cibernéticos praticados mundialmente se contrapõe ao número de soluções, o que denota o sentimento de injustiça das vítimas. Com o avanço tecnológico e a democratização da internet, a ocorrência de crimes cibernéticos aumentou a ponto de se tornar uma verdadeira epidemia global silenciosa, o que contrapõe o avanço da tecnologia pública a serviço da resolução destes crimes, pairando, portanto, a sensação de que a internet é uma "terra sem lei".

Vírus de computadores e programas com *malware* incluídos em pacotes de software ou arquivos aparentemente inofencivos são os meios mais comum através dos quais se praticam crimes ou violações digitais. A partir disso, por exemplo, se roubam perfis de redes sociais, acessam contas bancárias e fraudam cartões de créditos. Inobstante, quase nove em dez adultos reconhece a potencialidade da ocorrência de um crime cibernético, menos de um quarto espera ser vítima dele. No mesmo sentido, apenas metade se diz disposto a mudar sua forma de comportamento online para evitar tornar-se uma vítima. Paradoxalmente, apenas um em dez afirma se sentir muito seguro navegando online (NORTON, 2018).

A prática de crimes digitais também pode atingir o ambiente das empresas, seja violando segredos comerciais, usurpando banco de dados, expondo transações, etc. Neste sentido, o presente artigo se propõe a investigar as implicações da internet na vida do consumidor, sobretudo com relação à hiperbolização da vulnerabilidade quando este atua no ciberespaço, e à potencialização das violações aos direitos fundamentais frente ao ambiente virtual, relacionando a situação com os crimes cibernéticos.

O trabalho apresenta quatro seções, sendo a primeira acerca do surgimento e emergência do ciberespaço e do advento das Tecnologias da Informação e Comunicação (TIC's), com o intuito de apresentar o novo cenário em que se inserem as relações sociais por meio da internet. Após, insere-se a figura do consumidor e sua vulnerabilidade (*lato sensu*), equiparando-o ao *status* de usuário do meio virtual para então tratar dos crimes cibernéticos, as novas práticas e denominações, além das condutas igualmente lesivas que ainda não são tipificadas como crime, mas, igualmente, lesam direitos do consumidor (usuário). Ao cabo, expõe-se brevemente a problemática inerente à proteção de dados pessoais, demonstrando a importância da legislação firme para coibir práticas invasoras e lesivas, analisando as disposições da LGPD e as perspectivas após a vigência.

Para tanto, a metodologia empregada para abordagem se deu através do

método dedutivo, utilizando-se ainda pesquisas bibliográficas e revisão de literatura.

A emergência do ciberespaço e o advento das TIC'S

Antes de adentramos especificamente nas questões atinentes aos crimes digitais praticados em face consumidor, se faz necessária a compreensão do ciberespaço, já que esse se encontra intimamente relacionado ao desenvolvimento tecnológico das últimas décadas e é tido como o próprio espaço que proporciona a experiência digital.

Quando falamos em web ou em rede nos remetemos a uma ideia de cadeia interligada. Do latim *retis*, a rede se traduz em uma série de linhas ou fios que se entrelaçam e se sustentam (DIAS, 2005, p. 23). O sistema de redes é conhecido desde povos antigos, como os de civilizações pré-colombianas, que se utilizavam de sistemas de comunicação por estradas e pontes que serviam como junção de partes do Império (ROWE, 1946, p. 183-330) para, através de tais, passarem os mensageiros, trazendo e levando informações de outros povoados, o que se refletia em uma arcaica - mas complexa para a época - rede de comunicações.

Já no século XIX há uma profunda tranformação na comunicação em nível global através das redes informacionais decorrentes da criação do telégrafo e do telefone, sistema que permitiu a "aproximação" de locais distantes frente à nova compreensão do espaço-tempo que deles emergiam (HARVEY, 1993).

Em meados de 1940, com o avanço de indústrias eletro e microeletrônica, os pilares para solidificação da denominada "terceira revolução industrial" foram sendo criados, aliados a uma noção de progresso caracterizada pela tecnologia. Pouco tempo depois, foram se aperfeiçoando as indústrias automobilística, aérea e eletrônica com foco na computação, período em que se ampliam as redes de comunicação e aparecem os primeiros contornos do ciberespaço.

É a partir da década de 1970 que autores destacam que as tecnologias da informação "difundiram-se amplamente, acelerando seu desenvolvimento sinérgico e convergindo em um novo paradigma" (CASTELLS, 1999). Da invenção dos computadores na Segunda Guerra Mundial com o propósito de mera realização de cálculos às suas subsequentes evoluções tecnológicas marcadas pelo microprocessamento, destacamos a criação de mecanismos de linguagem de comunicação que permitiram a interação entre máquina e seres humanos, facilitando o uso por usuários comuns, mesmo os leigos em informática.

Refletindo sobre o assunto, Pierre Lévy aduzia que, a partir de 1980, a informática já vinha perdendo, pouco a pouco, o seu status meramente técnico e industrial, fundindo-se às telecomunicações (LÉVY, 1999) o que possibilitou, desde então, sua acelerada difusão pelo globo. Paralelamente a isso, com a expansão das

tecnologias de telecomunicações atrelado ao aperfeiçoamento microeletrônico, os microcomputadores passaram a ser (inter)ligados em redes de conexão e interação. Castells explica que:

> [...] essa capacidade de desenvolvimento de redes só se tornou possível graças aos importantes avanços tanto das telecomunicações quando das tecnologias de integração de computadores em rede, ocorridos durante os anos 70. Mas, ao mesmo tempo, tais mudanças somente foram possíveis após o surgimento de novos dispositivos microeletrônicos e o aumento da capacidade de computação, em uma impressionante ilustração das relações sinérgicas da revolução da tecnologia da informação (CASTELLS, 1993, p. 81).

Daí se tem a base para o que, no início da década de 1990, veio a se efetivar sob a denominação de internet ou rede global de computadores, popularizada e aberta a qualquer proprietário de um computador e uma linha telefônica pessoal (CASTELLS, 2003). O lançamento do conhecido sistema operacional Windows e a abertura de sistemas para desenvolvimento das TICs (Tecnologias de Informação e Comunicação), aliadas à difusão, principalmente social, da internet, influenciaram efetivamente a emergência do ciberespaço em que se vê realizada a sociedade informacional.

O crescimento e popularização da rede mundial de computadores, especialmente a partir do final do século XX para o início do século XXI, se caracteriza por um fluxo de informações através daquela rede jamais antes verificada na humanidade, sendo que as atividades exercidas ou facilitadas pelas tecnologias atreladas à internet penetraram o próprio meio de vida das pessoas, impactando das mais diversas maneiras na sociedade. Podemos dizer, conforme tratado por Castells, que a sociedade da informação está permanentemente incorporada à nossa sociedade, e vice-versa (CASTELLS, 2003). A interação e integração de computadores conectados através da rede internet possibilitou o surgimento de um novo espaço geográfico - o ciberespaço - materializado pelos meios de comunicação tecnológicos e interativos.

O conceito de ciberespaço surgiu inicialmente em 1894 e, embora ainda não existisse uma rede de internet que conectasse máquinas e pessoas pelo mundo, era tido como "um espaço não físico ou territorial no qual uma alucinação consensual pode ser experimentada diariamente pelos usuários" (TANCMAN, 2002). Em definição mais moderna, o ciberespaço foi tratado como "o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores" (LEVY, 1999, p.92). Tratar-se-ia, pois, de um espaço em uma dimensão imaterial que, segundo Marcondes Filho, seria:

> espaço imaterial tecnologicamente construído na camada eletromagnética do planeta e pressuposto entre computadores conectados por modem e fibras óticas […]. Tal espaço imaterial não tem, naturalmente, qualquer semelhança com o espaço geográfico.

> Trata-se de um espaçotempo, ou melhor, um espaço-velocidade […]; como tal, não pode ser provocado empiricamente, embora seja real. (MARCONDES FILHO, 1996, p. 100).

Há autores, todavia, que rechaçam essa conceituação ao argumento de que a mesma só faria sentido se o ciberespaço estivesse presente na camada eletromagnética do planeta (ionosfera), pois, de outro modo, deveria ser entendido como uma extensão do espaço geográfico (CRAMPTON, 2003, p. 10), reflexo de elementos contemporâneos da estrutura da própria sociedade. Pierre Lévy sugere que o ciberespaço é o terreno onde funciona a humanidade atualmente. Nessa esteira de ideias, Jemery Crampton também afasta a ideia transcendental do ciberespaço:

> Ao resistir a essas manobras eu sugiro que o ciberespaço é objetivado no nível errado de análise. A forma como o ciberespaço é tratado aqui não é transcendental (ou seja, como alguma "coisa" além de nós, que é "menos" real, ou, como para eXistenZ19, uma substituição do real), mas como um processo mútuo de produção entre espaço físico e espaço abstrato ou virtual, como uma série de relações, e como um processo de transformação (CRAMPTON, 2003, p. 12).

O ciberespaço se caracteriza pela convergência digital consubstanciada na integração de diversos formatos e dispositivos em um mesmo "lugar", ou seja, trata-se de um espaço conceitual inserido no ambiente das TICs. Assim, dada a continuidade dos avanços tecnológicos, atualmente o ciberespaço não pode ser visto tão somente como um espaço de interconexão de computadores, mas sim em todas as suas variações como tablets, smartphones, laptops, vídeos games, smartvs, etc, tornando uma característica desse espaço a multidisciplinaridade.

Consoante a emergência do ciberespaço, as novas relações sociais foram igualmente modificadas e as maneiras inovadoras de interação da vida cotidiana pela tecnologia evidenciam a "sociedade do conhecimento"[i]. Deste modo, as latentes alterações proporcionadas pela tecnologia confirmam que ela é hoje "o que a eletricidade foi na Era Industrial, em nossa época a Internet poderia ser equiparada tanto a uma rede elétrica quanto ao motor elétrico, em razão de sua capacidade de distribuir a força da informação por todo o domínio da atividade humana" (CASTELLS, 2003, p. 7).

Dessa maneira, a vivência humana tem sido alterada pelos desdobramentos das TICs, modificando e tornando mais complexas as relações sociais na era "Sociedade da Informação". Por fim, cumpre dizer que, no contexto em que novas demandas sociais são criadas, o acesso à internet é tido como um direito fundamental pela ONU (UNITED NATIONS, 2011), tornando a informação a chave para o desenvolvimento dos povos.

A vulnerabilidade no direito consumerista

Como pode-se observar, no mundo globalizado, as formas de consumo vêm sendo alteradas rapidamente, de modo que se faz imperioso promover a análise dos conceitos de consumidor e fornecedor para que se estabeleçam os limites de cada um, bem como de sua evolução dentro das novas formas de prestação de serviços e produtos, notadamente na internet. Desse modo, para que se compreenda o desenvolvimento de tais conceitos, importante se faz a indicação do que o Código de Defesa do Consumidor conceituou como consumidor. Segundo esse dispositivo legal, consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final (BRASIL, 1990).

De forma ampla, o parágrafo único do referido artigo equipara ao conceito de consumidor toda a coletividade de pessoas, ainda que indetermináveis, nos casos em que tiverem intervindo na relação de consumo. Ainda, se tratando do conceito de fornecedor, o Código de Defesa do Consumidor prevê em seu artigo terceiro:

> Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços (BRASIL, 1990, art. 3º).

Outrossim, o CDC se preocupou em apresentar os conceitos de produtos e prestação de serviços, além de demais dispositivos conceituais, todos com a finalidade de promover a proteção do consumidor, especialmente porque tido como um direito fundamental pela Constituição Federal.

Neste sentido, é harmônico o entendimento da doutrina no que diz respeito à noção de vulnerabilidade do consumidor para o Direito. Consoante destaca Behrnes (2014), a vulnerabilidade do consumidor é característica intrínseca das relações de consumo, constituindo-se ela, em presunção legal e absoluta a seu favor (BEHRENS, 2014, 309). Ou seja, tratado como um princípio no ordenamento pátrio, a vulnerabilidade do consumidor está intrinsicamente enquadrada na seara da defesa do consumidor, protegida tanto pela legislação especial, quanto pela imposição que a eleva a categoria de garantia constitucional, com a finalidade de constituir a ordem econômica do Estado brasileiro.

Neste sentido, o princípio da vulnerabilidade relaciona-se com a proteção do(s) indivíduo(s) no ambiente comercial, objetivando a aplicação de demais fundamentos legais como a isonomia, equidade e equilíbrio das relações contratuais sendo, portanto, a vulnerabilidade caracterizada como uma fonte de direito, gozando de respaldo jurídico para sua efetivação (SOUZA; ALVES).

Com todo o aparato protetivo, o Estado passa a exercer sua função jurisdicional enquanto um agente de controle para que as relações de consumo sejam pautadas não pela desigualdade entre sujeitos, mas pela adequação das relações, visando o equilíbrio entre as esferas econômicas, técnicas e judiciais.

Ressalta-se ainda que o Código de Defesa do Consumidor faz distinção entre os termos "vulnerabilidade" e "hipossuficiência". A primeira corresponde unicamente ao direito material, circunstância inerente à condição de consumidor. Já a hipossuficiência diz respeito à desigualdade no âmbito processual, devendo esta ser averiguada de acordo com o caso concreto, tendo em vista que não é presumida.

Segundo alguns autores, o princípio da vulnerabilidade é dividido em três aspectos, quais sejam, a vulnerabilidade técnica, científica e fática (MIRAGEM, 2016). Isto porque tal princípio é multiforme, devendo ainda ser levado como base a categoria da vulnerabilidade informacional, principalmente nas formas de consumo virtuais, como será tratado adiante.

A vulnerabilidade técnica corresponde à condição do consumidor em não conter informações precisas acerca daquilo que compra, sendo presumido que o fornecedor detenha tais informações específicas sobre aquilo que comercializa. Já a vulnerabilidade jurídico-científica demonstra a ideia de que o consumidor nem sempre tem conhecimento de todos os seus direitos. De modo que a vulnerabilidade jurídica-cientifica é presumida nos casos em que o consumidor for pessoa física (MIRAGEM, 2016).

Segundo acertadamente preleciona Beherns (2014), o consumidor não tem informações suficientes para saber quais seus direitos, como funciona sua proteção contratual e quais órgãos contatar, no caso de descumprimento contratual ou acidente de consumo (BEHRENS, 2014, p. 311), demonstrando, mais uma vez, a necessidade da proteção massiva ao consumidor nas relações de consumo.

Em sequência, a vulnerabilidade fática diz respeito à relação de consumo em concreto. Caracteriza-se pela desigualdade financeira entre o consumidor e fornecedor, tendo em vista o poder econômico superior daquele que produz, principalmente se tratando de relação de consumo entre pessoa física e jurídica.

Além de todo o exposto, mister destacar que, assim como a maioria das relações interpessoais existentes na sociedade, o desenvolvimento das relações de consumo também vem se modificando ao longo do tempo, tendo esta última ganhado grande avanço em um pequeno espaço temporal.

Neste sentido, a sociedade encontra-se cada vez mais conectada por meio da internet, com amplo acesso à informação, conhecimento e lazer e, especificamente, às relações de consumo. Isto se dá, principalmente, porque comumente restringimos a

relacionar o direito do consumidor objetivamente à compra e venda, não levando em consideração a troca de informações por meio de redes sociais, o fornecimento de dados às empresas e o recebimento de propagandas, por exemplo. Para Ucar:

> O público se conecta às redes sociais para estabelecer novas formas de relacionamento e se engajar de forma colaborativa no ambiente da produção midiática. Neste sentido, o consumidor tem à disposição mecanismos para organizar sua própria grade de consumo midiático e pode optar por suprimir a propaganda. Por outro lado, o consumidor on-line também ganha ferramentas que o aproxima de seus produtos e personagens favoritos, o que aumenta as demandas de engajamento na rede (UCAR, 2016, p.126).

Diante do exposto, percebe-se que as redes sociais e a rede mundial de computadores, de forma geral, permitem interações multifacetadas e eletivas, gerando a possibilidade de indivíduos popularizarem serviços das mais diversas áreas. Corroborando este entendimento Carvalho explica que:

> O uso de mídiassociais conectadas pelas empresas é tema recorrente no meio empresarial e social. Em evento promovido pela Câmara Oficial Espanhola de Comércio no Brasil, no dia 9 de novembro, esse tema foi abordado por Ronaldo Tano, gerente de consultoria empresarial da Deloitte. Segundo ele, as empresas precisam se voltar para as mídias sociais, especialmente pela geração colaborativa de conteúdo que cresce de forma rápida e consistente. Tano propôs que o "o uso das mídias sociais seria uma construção de redes colaborativas para que as companhias conheçam seus clientes", principalmente no monitoramento da marca. Em sua apresentação, destacou que cada empresa pode construir sua própria abordagem e sugere que isto se faça com três verbos: atrair, ajudar e afiliar, o que exige o envolvimento da alta direção da empresa e a disponibilidade de recursos suficientes. Para ele, as empresas precisam conhecer o conceito de inteligência online, para que saibam o que fazer com as informações obtidas por meio das redes sociais (CARVALHO, 2012, p.5).

Diante da exposição do tema, resta claro que a conhecida "era da internet" modificou a relação entre as pessoas e, consequentemente, a relação de consumo entre os indivíduos. Inicialmente criada com o propósito de fomentar o relacionamento virtual entre pessoas, as redes sociais e a internet de modo geral, se transformaram em um grande espaço a ser explorado por empresas e prestadores de serviços com a finalidade de fomentar o consumo e o lucro.

Assim, imperioso questionar o papel e as características que o consumidor virtual passa a assumir diante de tantas modificações. A partir da falta de informação e despreparo técnico e intelectual do consumidor frente aos negócios pactuados de forma online, busca-se desenvolver uma aplicação da exegese protetiva do Código de Defesa do Consumidor às contratações eletrônicas. Isto porque, embora a relação de

consumo permaneça a mesma em sua essência, no comércio eletrônico, o consumidor perde todos os referenciais a que está acostumado, tornando-o ainda mais vulnerável dado o estranhamento tecnológico.

Vale ressaltar que a vulnerabilidade do consumidor no meio eletrônico não deve ser restrita somente à falta de proficiência informática, mas também à ausência de saberes básicos quanto à compreensão da tecnologia utilizada. Segundo a professora Claudia Lima Marques, a posição de vulnerabilidade do consumidor é aumentada ainda mais, uma vez que a produção se despersonalizou totalmente, tornando-se mundial. Ainda conforme a autora, o mundo virtual modificou os hábitos de consumo e o tempo, expandindo as possibilidades de publicidade, agravando os conflitos de consumo e a própria vulnerabilidade informacional, fática e jurídica do consumidor (BENJAMIN, 2013).

Diante da falta de informação e despreparo técnico acerca dos contratos de consumo realizados, os consumidores virtuais passaram a ser vulneráveis não somente diante da relação material que é promovida por meio de compra de produtos ou serviços tradicionais, mas principalmente diante das empresas virtuais e pessoas dispostas a utilizarem a plataforma digital para aplicar golpes e utilizarem-se de dados não protegidos pelo fornecedor.

A exacerbação da vulnerabilidade tornou-se tão notória diante dos mais diversos contratos de adesão pelos quais são obrigados a aceitar, informando seus dados pessoais e demais informações, que diversos mecanismos de proteção, para além do código do consumidor têm sido criados. A Lei Geral de Proteção de Dados demonstra a necessidade de reafirmação do Princípio da Vulnerabilidade no ciberespaço e a tutela dos indivíduos enquanto consumidores virtuais.

Os crimes cibernáticos na Socieddae do Conhecimento

Tendo a tecnologia se atrelado à vida das pessoas a ponto de ser considerada essencial em todos os anseios sociais, é preciso refletir acerca das implicações negativas, notadamente no surgimento de novos crimes a partir do ciberespaço.

No Brasil, uma das primeiras legislações aplicadas à informática foi a Lei da Informática (Lei 7.646/87) que, inclusive, recebeu esse nome por ter sido "a primeira a tipificar uma conduta que, embora assemelhada à violação de direito autoral, constituía um crime informático em sentido próprio declarado expressamente que o regime de proteção à propriedade intelectual de programas do computador era o direito do autor" (LUCCA; SIMÃO FILHO *et al.*, 2001, p. 226). Posteriormente, a Lei n. 9.609/98 dispôs sobre a propriedade intelectual na rede de computadores atinentes aos direitos autorais de obras literárias[ii].

Com a popularização da internet, diversas novas condutas lesivas passaram a ser perpetradas no (e através do) ciberespaço sem que existisse regulamentação legal que pudesse conferir uma proteção ou resposta para os novos desdobramentos virtuais.

O distanciamento dos indivíduos do mundo real proporcionado pela barreia virtual, aliado à falta de regulamentação e proteção do espaço cibernético aos usuários, trouxe a lume a possibilidade de que novos crimes fossem praticados nesse meio, lesando, sobremaneira, seus consumidores. Queremos dizer, pois, que o indivíduo não precisaria mais sair às ruas para delinquir e atingir o patrimônio, privacidade honra, dentre outros, do cidadão, pois a internet se apresenta como um instrumento facilitador para tanto. Neste sentido:

> Alguns fatores como a intensificação dos relacionamentos via internet, a produção em série de computadores, a popularização do comércio eletrônico (e-commerce) e o aumento de transações bancárias, estão diretamente ligados ao aumento de ocorrências de crimes conhecidos, mas que praticadas pela internet ao surgimento de novos valores e logicamente à novas condutas delitivas (BRITO, 1999, p.14).

Os crimes cibernéticos ou crimes de informática podem ser classificados como condutas que atentam contra dados e contra o computador (e através dele), ou seja, são aqueles "crimes relacionados às informações arquivadas ou em trânsito por computador, sendo esses dados acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico" (CORREA, 1999, p. 43).

A título de exemplo, em 2001 o então Procurador da República na Bahia, Vladimir Aras, já advertia acerca da preocupação com os prejuízos por parte das empresas frente a ocorrência de crimes digitais:

> as perdas com fraudes no ano passado atingiram R$200 milhões. No ano anterior, o prejuízo foi de R$ 260 milhões e, em 1998, de R$300 milhões". A Abecs tem se preocupado com os cibercrimes praticados mediante o uso fraudulento de cartões de crédito e está introduzindo no mercado os cartões com chips eletrônicos, que têm alto nível de segurança (ARAS, 2001, p.28).

Denota-se que o Direito se encontra diante uma nova realidade que exige novos contornos legislativos na proteção dos consumidores conectados ao ciberespaço. Note-se que os crimes cibernéticos muitas vezes encontram resistência na sua resolução justamente em razão da dificuldade de identificação do autor, que geralmente pratica o crime anônimo, ou, ao menos, "distante" do local em que o mesmo se consuma. Frise-se que essa dificuldade não é encontrada somente no Brasil, mas no mundo todo. Ademais, os crimes cibernéticos costumam exigir de seus autores certos conhecimentos específicos para a própria empreitada criminosa, o que acaba

por contribuir para que detenham igual expertise para ocultar os seus rastros online.

Hoje a literatura trabalha como algumas denominações para os cibercriminosos, conforme passaremos, resumidamente, a expor, asseverando que não são esses os únicos, mas sim os mais conhecidos.

Inicialmente cumpre apontar que a nomenclatura mais conhecida, *hacker*, não indica necessariamente algo ruim. O *hacker*, cujo termo se relaciona com a ideia de "pirata", embora possa invadir sistemas, não pratica condutas delituosas ou lesivas, sendo que, ao contrário, por vezes utiliza de suas habilidades para criar e desenvolver sistema mais seguros. De outro lado, o *cracker* possui igualmente o conhecimento técnico do *hacker*, mas atua visando o prejuízo alheio, ou seja, ao quebrar o sistema de segurança e invadi-los, o *cracker* busca a captação de dados que possam lhe render lucros. Aliás, o termo *cracker* foi criado pelos próprios *hackers*, em defesa da classe contra o uso jornalístico indevido da palavra. Já o *carder* pode ser visto como um estelionatário virtual, que se aproveita de falhas nos sistemas de seguranças de empresas ou da vulnerabilidade de consumidores para criar programas que realizem compras, utilizando-se de dados alheios obtidos ilegalmente (ROCHA, 2013).

De grande repercussão nacional, o caso "Carolina Dieckmann" reflete a atuações de *crackers* e a ausência de legislação protetiva adequada. Na ocasião, criminosos invadiram o computador da atriz global Carolina Dieckmann e, de posse de suas credenciais, conseguiram acesso a fotografias íntimas e privadas, expondo-a através da comercialização desse conteúdo, inclusive com sites pornográficos. Pela repercussão midiática, os autores acabaram presos, mas, em razão inexistência de legislação específica, acabaram indiciados por furto sob grande crítica da comunidade jurídica em razão de eventual aplicação de norma penal incriminadora por analogia.

Fato que nos interessa é que, após esse episódio, foi sancionada a "Lei Carolina Dieckmann", Lei 12.737/12, que incluía no Código Penal tutela de dispositivo informático[iii], além de acrescer ao Art. 286 do mesmo Diploma Legal parágrafo que consideraria igual crime a conduta de interromper serviço telemático ou de informação. No mesmo sentido, equiparou o cartão de crédito e de débito a documento particular para fins de incidência no tipo penal do artigo 298 do Código Penal[iv] , como a conduta de clonar um cartão.

Cumpre registrar, todavia, que a referida lei não significa necessariamente o fim de crimes cibernéticos, seja em razão da impossibilidade do processo legislativo acompanhar o avanço tecnológico, seja porque alterações na legislação penal não tratam de condição *sine qua non* para combater e coibir crimes frente à própria função do Direito Penal. Ademais, a inovação criminológica que acompanha a evolução do ciberespaço requer muito mais do que legislações que regulamentem condutas criminosas.

Não pretendemos aqui nos aprofundar em questões de direito material ou processual penal, mas sim expor como se agrava a vulnerabilidade do consumidor frente à intensificação da utilização da internet e armazenamento cada vez maior de dados dos usuários, o que contribui para o aumento no número de cibercrimes que atentam contra direitos fundamentais. Note-se, por oportuno, que embora nos refiramos a "crimes", o fazemos de maneira geral (*lato sensu*), pois existem diversas condutas questionáveis, comissiva ou omissivas, praticadas por particulares, empresas e provedores que, eventualmente, podem lesar igualmente o consumidor ainda que não sejam tipificadas como crime.

Assim, não são somente condutas tipificadas como crimes podem lesar direitos do consumidor no âmbito do ciberespaço, mas também condutas que se relacionem com armazenamento, tráfego, cessão e compartilhamento de dados dos usuários de bens e serviços digitais, especialmente diante dos novos contornos que tratam de dados como fonte de riqueza e de poder (SIMÃO FILHO; SCHWARTZ, 2016, p. 313).

As perspectivad da LGPD

O direito de acesso à informação se relaciona com dois direitos fundamentais: o da garantia à privacidade (Art. 5, inciso X, da Constituição Federal) e o direito à informação (Art. 5, inciso XIV, da mesma Lei Maior). Nos dias atuais, a informação é tida como uma nova espécie de matéria prima que corresponde a um "elemento estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade [...]" (BIONI, 2019, p.87), sendo, atualmente, capaz de gerar renda àqueles que a tratam e a transformam em dados estruturados capazes de demonstrar a viabilidade de um produto, o alcance de uma propaganda, o interesse do público alvo, etc.

Parte-se da ideia de que os dados e informações das pessoas podem ser transformados em produtos a serem vendidos através de uma publicidade direcionada por sistemas e algoritmos que filtram a propaganda e entregam ao consumidor em potencial, daí seu potencial de mercado.

Recente pesquisa realizada em março de 2019 pela Serasa Experian aponta que 75% dos brasileiros desconhecem ou conhecem pouco sobre a Lei de Proteção de Dados. A novel normativa é tida como um marco jurídico-regulatório na legislação brasileira que, após sucessivos adiamentos, passou a viger em meados de setembro de 2020 (SERASA). A respeito do assunto, Bioni afirma que:

> Os dados pessoais de um indivíduo formam um perfil a seu respeito para a tomada de inúmeras decisões. […]. Na famosa expressão de Eli Pariser, há uma bolha que, como um filtro invisível, direciona desde a própria interação do usuário com outras pessoas em uma rede social até o acesso e a busca por informação na rede. Doutrina-

> se a pessoa com um conteúdo e uma informação que giram em torno dos interesses inferidos por intermédio dos seus dados, formando-se uma bolha que impossibilita o contato com informações diferentes (BIONI, 2019, p.93).

Neste sentido, embora não tenhamos o objetivo de aprofundar o estudo sobre proteção de dados no presente artigo, faz-se necessário compreendê-lo à luz da vulnerabilidade do consumir no ciberespaço, o que pode facilitar ainda mais a exposição da privacidade e intimidade do cidadão em um espaço com poucas regras, permitindo o uso indevido por pessoas e empresas mal intencionadas.

Bioni (2019) ainda explica que, sendo a maioria dos conteúdos disponibilizados gratuitos na internet e, portanto, distante do padrão de consumo normal onde é exigida uma contraprestação pelo produto ou serviço adquirido, dentro do ciberespaço as empresas têm se aproveitado para tratar o usuário como produto e seus dados como a contraprestação imposta (BIONI, 2019).

A maioria dos dados inseridos pelos consumidores no ciberespaço se dá através de simples contrato adesão para criação de uma "conta" ou "perfil" de usuário, no qual ele é obrigado a exarar seu aceite aos longos "Termos de Uso" ou "Política de Privacidade", aceitando, na maioria das vezes, imposições unilaterais que o consumidor sequer imagina consentir. Vale dizer, todavia, que esse tipo de adesão se afigura viciada "seja porque ele reforça a aventada assimetria do mercado informacional, seja porque se trata de uma ferramenta que não capacita, efetivamente, o cidadão para exercer controle sobre suas informações pessoais" (BIONI, 2019, p.32).

Os dados ficam armazenados no Big Data, que seria um resultado total de todos os meios de coleta de dados reunidos em um só "lugar". Pode ser explicado enquanto um:

> conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores (ITS, 2016, p.47).

Em exemplo de fácil compreensão, as respostas do Big Data são utilizadas para sugerir novos amigos na rede social Facebook, para indicar sugestões de compras nas propagandas nas laterais das páginas ou das pesquisas do Google, baseando-se nos dados obtidos a partir da sua navegação ou dos já fornecidos por empresas.

Em 2018 o mundo também se viu abalado pelo escândalo de vazamento de dados do Facebook-Cambridge Analytica, em razão da coleta e utilização indevida de dados para fins de orientar a posição política em eleições de cerca de 87 milhões de usuários daquela rede. Na ocasião, o CEO do Facebook, Mark Zuckenberg, teve de se dirigir ao Congresso Americano e se desculpar pelo episódio classificado como "erro"[v].

A complexidade e infinitude dos dados inseridos no universo da internet pode implicar incontáveis desdobramentos e práticas lesivas aos consumidores. Pode-se saber, por exemplo, a partir do armazenamento de dados de geolocalização pelo aplicativo Google Maps, que se encontra vinculado a uma conta Google, os locais que o usuário frequentou; o caminho que faz para se dirigir ao trabalho; o tempo em que permaneceu em um local, etc.

Advertimos, assim, que o consumidor dos serviços digitais, vítima da colheita indiscriminada, permanente e silenciosa de seus dados, não sabe da ocorrência dessa prática ou sequer possui os meios necessários para ter conhecimento dos resultados ou para conseguir interromper ou cancelá-los. De mais a mais, sequer seria possível saber com quantos outros sites, provedores ou empresas, e por quantas vezes, um mesmo dado foi compartilhado, ou seja, uma vez obtido um dado, torna-se praticamente impossível controlá-lo.

Chamamos atenção para as incontáveis possibilidades de violação a direitos fundamentais dos consumidores, inclusive, de modo a atingir bens jurídicos tutelados penalmente, através da exposição e facilidade decorrente do uso indiscriminado da internet e da negligência e abuso por partes dos provedores e fornecedores de bens e serviços online.

Outrossim, a Lei Geral de Proteção de Dados Pessoais, regida pela Lei 13.709/2018 ainda não em vigor, visa dar um melhor tratamento aos dados pessoais no ciberespaço. Brevemente, a referida Lei tem por escopo garantir ao consumidor/usuário pleno direito de consentir ou não a coleta de seus dados com o fim de proteger os direitos fundamentais de liberdade e de privacidade, além do livre desenvolvimento da personalidade (BRASIL, 2018).

Embora sejam indiscutíveis os avanços que a LGPD permitirá no manejo dos dados pessoais, entendemos que o legislador perdeu a oportunidade de inserir na legislação condutas típicas que pudessem aumentar a zona de proteção eficiente do consumidor. Portanto, em que pesem as novas responsabilidades atribuídas às empresas e órgãos que detenham os dados legalmente, ainda haverá aqueles que se utilizarão de dados obtidos legalmente para lesar o consumidor com a prática de cibercrimes, pois, ainda que os dados tenham sido obtidos seguindo-se a lei, a proteção pode ser deficiente para fins de coibir crimes. Cumpre recordar que, embora o uso das TICs seja algo benéfico à sociedade, não há como negar que a maioria dos sites e aplicativos não visam promover a inclusão digital ou a melhora da vida das pessoas, mas sim meramente o intuito de obter lucro, o que acaba por vulnerabilizar o consumidor.

Conclusão

Observou-se, no trabalho, que as relações humanas tiveram significativas mudanças após o advento da internet e das TICs, notadamente em relação aos meios decomunicação e informação. As distâncias físicas entre lugar e indivíduos se tornaram barreira transponível para muitas atividades sociais e comerciais e, paradoxalmente, frente ao uso indiscriminado por particulares, o mundo "real" parece cada vez mais distante, dada a importância da vida online.

Com o advento e solidificação da denominada Sociedade da Informação, o antigo paradigma de acúmulo de riqueza através de bens materiais suscetíveis de atribuição de valor em dinheiro passou a ser relativizado, dando lugar à relevância de bens imateriais, como quantidade de usuários, seguidores e, principalmente, acerca de dados pessoais. Vale registrar que mesmo os dados aparentemente mais inofensivos e insignificantes podem ser valiosos e igualmente perigosos quando cruzados com outras fontes, inclusive porque não há como prever quando e com qual finalidade o mesmo poderá vir a ser utilizado.

A sociedade 4.0 decorrente da revolução tecnológico e a rede de internet aberta e acessível facilitaram a disseminação de infinitas possibilidades, porém sem ser acompanhada por legislações e práticas que as adequassem à proteção de bens jurídicos fundamentais. Ora, ainda que o ciberespaço seja um novo ambiente social, modificado e atualizado segundo a segundo, deve ser entendido como uma extensão do espaço geográfico, razão pela qual deve possuir iguais regras de convivência.

As condutas das empresas em armazenar, analisar e compartilhar dados visando lucro expõem ainda mais o consumidor vulnerável, sendo que a web se tornou um cenário de agravamento daquela situação, ou seja, o consumidor, diante da falta de regras específicas, negligência das empresas e provedores, e pouca noção de segurança torna-se presa hipervulnerável, seja em relação ao mercado publicitário e financeiro ou a criminosos virtuais.

A pesquisa demonstrou ainda que, embora a internet tenha se expandido sobremaneira, as formas de combate aos crimes cibernéticos ainda são precárias, sendo poucas as condutas tipificadas efetivamente como crimes. Outrossim, diante da nova perspectiva de análise, armazenamento e gestão de dados pessoais, entendemos que o consumidor, inobstante discussões para sua proteção, se encontra cada vez mais vulnerável justamente em razão da importância atribuída a suas informações. Isso é, embora as empresas tenham de agir eticamente em posse de dados pessoais, podem estar a preparar o terreno para atuação mais incisiva de cibercriminosos.

O crime online difere-se do crime "real" justamente por seu pouco tangível ou visível para a maioria das pessoas e autoridades, se fixando como de difícil solução. Assim, a crescente informatização em rede pelo mundo tem gerado diversas melhoras e facilidades na vida das pessoas, mas, ao mesmo tempo, a toda facilidade corresponde

um afrouxamento de postura por parte dos usuários, de tal modo que tem igualmente atraído olhares daqueles detentores de elevado conhecimento tecnológico que se utilizam desse instrumento para obter vantagens ilícitas através de crimes cibernéticos.

Dados pessoais devem ser vistos hoje não só como fonte de riqueza, mas, sobretudo, fonte de poder, notadamente para fins de controle da sociedade. Assim, frente à ausência de proteção dos consumidores online, a internet pode ser um meio de violação de direitos fundamentais.

Referências

ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. **Jus Navigandi**, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: < https://jus.com.br/artigos/2250/crimes-de-

informatica>. Acesso em: 12 de out. 2020.

BBC. **Facebook scandal "hit 87 million users**. Disponível em: <http://www.bbc.com/news/technology-43649018>. Acesso em: 12 de out. 2020.

BEHRENS, Yan West. **Comércio eletrônico de produtos e serviços**: uma análise das principais práticas abusivas em prejuízo dos consumidores. Salvador: Paginçe, 2014.

BENJAMIN, Antônio Herman Vasconcellos *et al.* **Manual de direito do consumidor**. 5. ed., ver., atual. e ampl. São Paulo: Revista dos Tribunais, 2013.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Ed 1. Vol. único. Rio de Janeiro: Forense, 2019

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 12 de out. 2020.

BRASIL.**Decreto Lei n 2.848** de 07 de novembro de 1940. Código Penal Brasileiro.

BRASIL.**Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

BRITO, Auriney Uchôa de. O bem jurídico-penal dos delitos informáticos. **Boletim IBCCRIM**: São Paulo, ano 17, n. 199, p. 14-15, junho 2009.

CARVALHO, Cláudio Luiz de. **O uso de redes sociais conectadas no processo de comunicação interna**. Dissertação (mestrado) –Faculdade Cásper Líbero, Programa de Mestrado em Comunicação –São Paulo, 2012. Disponível em: <https://casperlibero.edu.br/wp-content/uploads/2014/02/08-O-uso-de-redes-conectadas.pdf>. Acesso em: 12 de out. 2020.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz & Terra, 1999.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Editor, 2003.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 1999.

CRAMPTON, Jeremy W. **The political mapping of cyberspace**. Chicago: The University of Chicago Press, 2003.

CRAWFORD, Susan. **The origin and development of a concept**: the information society. Bull. Med. Libr. Assoc.. 71(4) October, pp. 380-385. Disponível em: <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC227258/pdf/mlab00068-0030.pdf>. Acesso em: 12 de out. 2020.

DIAS, Leila Christina. Os sentidos da rede: notas para a discussão. In.: DIAS, Leila Christina e SILVEIRA, Rogério Leandro Lima da. **Redes, sociedades e territórios**. Santa Cruz do Sul: EDUNISC, 2005.

HARVEY, David. **A condição pós-moderna**. São Paulo: Loyola, 1993.

ITS (INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO). Big Data no projeto Sul Global. **Relatório de estudos**. Rio de Janeiro: 2016. Disponível em: <https://itsrio.org/wp- content/uploads/2017/01/ITS_Relatorio_Big-Data_PT-BR_v2.pdf.> Acesso em: 12 de out. 2020.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coordenadores) e outros. **Direito & Internet**. Aspectos Jurídicos Relevantes. 1 ed. Bauru, SP: EDIPRO, 2001.

MARCONDES FILHO, Ciro. **Pensar - pulsar**: cultura comunicacional, tecnologias, velocidade. São Paulo: Edições NTC, 1996.

MIRAGEM, Bruno. **Curso de Direito do Consumidor**. 6. ed. São Paulo: Revista dos Tribunais, 2016.

MORAES, Fernando Dreissing de. Ciberespaço entre as redes e o espaço geográfico: algumas considerações teóricas. **Revista Caminhos de Geografia**. Instituto de Geografia da UFU. Disponível em: <http://www.seer.ufu.br/index.php/caminhosdegeografia/article/view/21779/13397.> Acesso em: 12 de out. 2020.

NORTON. **Relatório de Crimes Cibernéticos NORTON**: O impacto humano. Disponível em: < https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/N orton_Portuguese-Human%20Impact-A4_Aug18.pdf.> Acesso em: 12 de out. 2020.

ROCHA, Carolina Borges. A evolução criminológica do Direito Penal: aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. **Jus Navigandi**, Teresina, ano 18, n. 3706, 24 ago. 2013. Disponível em: <http://jus.com.br/artigos/25120>. Acesso em: 12 de out. 2020.

ROWE, John Howland. Inca Culture at The Time of The Spanish Conquest. In. STEWARD, Julian H. Handbook of South American Indians. Smithsonian Institution Bureau of American Ethnology, **Bulletin 143**. Washington: United States Government Printing Office, 1946. p. 183-330.

SERASA. Serasa Experian. 75% dos consumidores desconhecem ou conhecem pouco sobre a Lei de Proteção de Dados. Disponível em: <https://www.serasaexperian.com.br/sala-de- imprensa/75-dos-consumidores-desconhecemou-conhecem-pouco-sobre-a-lei-de-protecao-de- dados-revela-pesquisa-

inedita-da-serasa-experian.> Acesso em: 12 de out. 2020.

SIMÃO, Adalberto Filho. SCHWARTZ. Germano Andre. "Big Data" Big Problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. **Conpedi Law Review**. V.2, n.3, p. 311-331. 2016.

SIMÃO FILHO, Adalberto; PEREIRA, Sergio Luiz. Em busca dos reflexos da nova empresarialidade e da ecoeconomia nos direitos transindividuais. In: **Anais do IV Congresso Brasileiro de Processo Coletivo e Cidadania da Universidade de Ribeirão Preto.** n. 4, p. 58-84, out/2016. Disponível em: http://revistas.unaerp.br/cbpcc/article/view/720> Acesso em: 12 de out. 2020.

SILVA, Guilherme Carvalho da. **O Ciberespeço como categoria geográfica**. Dissertação de Mestrado em Geografia. Universidade de Brasília. 2013. Disponível em:<https://repositorio.unb.br/bitstream/10482/14214/1/2013_GuilhermeCarvalhoSilva.pdf.> Acesso em: 12 de out. 2020.

SOUZA, Thaiane Almeida; ALVES, Sérgio Emílio Schlang. **A Proteção ao Consumidor no âmbito do comércio eletrônico:** uma análise à luz do princípio da vulnerabilidade. Disponível em: <http://ri.ucsal.br:8080/jspui/bitstream/prefix/626/1/TCCTHAIANESOUZA.pdf.> Acesso em: 12 de out. 2020.

TANCMAN, Michele. **A (Ciber) Geografia das Cidades Digitais**. 2002. Dissertação de Mestrado em Geografia. Programa de Pós-Graduação em Geografia, Universidade Federal Fluminense, Rio de Janeiro, 2002.

UCAR, Bruna Santana. **A publicidade no Brasil**: agências, poderes e modos de trabalho (1914–2014). Orientador: Everardo Pereira Guimarães Rocha. Tese de Doutorado. Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Comunicação Social, 2016. Disponível em: <https://www.maxwell.vrac.puc-rio.br/27769/27769.pdf.> Acesso em: 12 de out. 2020.

UNITED NATIONS. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**. Disponível em: < https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>. Acesso em: 12 de out. 2020.

Notas:

[i] O conceito de "sociedade do conhecimento" foi primeiramente invocado por Fritz Machup, em 1962, na obra *The Production and ditribution of knolege in the USA,* e posteriormente desenvolvido por Peter Ducker, em 1966, na obra *The age of discontinuity* (CRAWFORD, 1983, p. 380).

[ii] *Cf.* BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD**). Lei nº 13.709, de 14 de agosto de 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 12 de out. 2020.

[iii] 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 (BRASIL, 1940).

[iv] *Cf*. BRASIL. **Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos**; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

[v] *Cf*. BBC. **Facebook scandal "hit 87 million users**". Disponível em: http://www.bbc.com/news/technology-43649018>. Acesso em: 12 de out. 2020.

Recebido em: nov.2020

Aceito em: dez.2020