A APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS E DA METODOLOGIA PRIVACY BY DESIGN NOS TERMOS DE USO E DE POLÍTICA DE PRIVACIDADE NO BRASIL

Gabriel Capparelli Haddad 1[1], Ms. Carlos Danilo Gaioli Euzébio[1]

[1]Faculdade de Tecnologia de FATEC Ribeirão Preto (FATEC)

Ribeirão Preto, SP – Brasil

mailto:gahaddad1@gmail.com, carlos.euzebio@fatec.sp.gov.br

Resumo. *A nova era da digital e a chegada da informática no cotidiano das pessoas fez com que muitas facilidades fossem criadas, porém certas facilidades necessitam de leis e fiscalizações para que sejam aplicadas de forma segura e clara, como é o caso dos contratos digitais, e a proteção de dados de usuários desses meios digitais, com base nessa pontualidade, a Aplicabilidade da Lei Geral de Proteção de Dados e da Metodologia Privacy By Design nos Termos de Uso e de Política de Privacidade, visa demonstrar que o comércio eletrônico e os contratos feitos por meios digitais precisam ser fiscalizados e auditados, a fim de se coibir os abusos por parte das empresas e proteção as partes mais vulneráveis.*

Abstract. *The new era of digitality and the arrival of information technology in people's daily lives meant that many facilities were created, but certain facilities need laws and inspections so that they are applied safely and clearly, as is the case with digital contracts, and data protection of users of these digital media, based on this punctuality, the Applicability of the General Data Protection Law and the Privacy By Design Methodology in the Terms of Use and Privacy Policy, aims to demonstrate that electronic commerce and contracts made by Digital media need to be inspected and audited in order to curb abuses by companies and protect the most vulnerable parties.*

1. Introdução

A nova constituição brasileira, promulgada no ano de 1988, trouxe para o Brasil um novo regime democrático, com novos direitos e deveres para o cidadão, em que a liberdade foi introduzida depois de anos de ditadura militar no Brasil. Com isso, o direito à vida e a liberdade de expressão passaram a fazer parte dos direitos fundamentais inerentes a vivência humana (BRASIL, 1988).

Com o passar dos anos e o surgimento da *Internet*, essa democracia e liberdade de expressão se tornaram mais ativas e presentes, com uma aparente harmonia entre a privacidade e a livre iniciativa, passando a explorar os dados pessoais como um item fundamental para o consumismo.

Zuboff (2019) mostra que a experiência humana no mundo digital, se tornou insumo para se verificar os parâmetros comportamentais de cada indivíduo. O autor ainda complementa que uma parte das informações que as empresas buscam é para o

aperfeiçoamento de produtos e serviços, mas uma grande parte serve para compor estudos que farão previsão das necessidades desses usuários, denominado como *machine intelligence* (inteligência da máquina).

Com essas informações captadas, as empresas conseguem filtrar informações que criam bases para se moldar um padrão comportamental futuro (ZUBOFF, 2019). E esse novo manejo de dados permite que as empresas tenham o poder sobre um consumidor vulnerável, com suas informações sendo repassadas de forma ilícita, havendo assim uma necessidade de proteção a esse consumidor, para se ter um equilíbrio em sua relação comercial.

O consumidor permite que suas informações pessoais fiquem mais vulneráveis em contratos denominados contratos por cliques, conhecidos como "vis á vis", em que os contratos físicos acabam partindo para o mundo digital, causando assim uma aceleração cada vez mais rápida, diminuindo não só tempo, mas também distância, porém com mais vulnerabilidade de exposição de dados dos consumidores.

Diante desse problema criado com o surgimento da nova era digital, é criada a Lei Geral de Proteção de dados (LGPD), Lei 13.709/18, que visa garantir a segurança dos dados das pessoas em ambientes virtuais, com o intuito de trazer maior autonomia aos usuários quanto a utilização de seus dados por empresas que operam de maneira eletrônica. As exigências da LGPD valem tanto para as lojas físicas quanto para virtuais, situadas no país ou no exterior que ofereçam serviços para pessoas no Brasil. Desta forma, as empresas deverão se adaptar a esta nova realidade através da contratação de profissionais: (DPO Data Protection Officer) encarregado, os controladores, os operadores e agentes de tratamento de dados, para tratar dos dados sensíveis de seus clientes através de ferramentas adequadas de T.I para garantir que haja o cumprimento da legislação vigente.

2. Metodologia

Este trabalho foi elaborado através de uma pesquisa exploratória e descritiva, Gil (2002) explica que pesquisa exploratória visa proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito. Os dados recolhidos foram de natureza essencialmente bibliográfica e documental. A pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos (GIL, 2002).

Pode-se dizer que uma pesquisa descritiva é uma das classificações da pesquisa científica, onde seu objetivo é descrever as características de uma população, um fenômeno ou experiência para o estudo realizado. Ela é realizada considerando os aspectos da formulação das perguntas que norteiam a pesquisa, além de estabelecer também uma relação entre as variáveis propostas no objeto de estudo em análise. (GIL, 2002). A pesquisa bibliográfica objetiva informações dadas a partir de materiais já existentes sobre o assunto, em livros, revistas, web sites, sendo assim, a pesquisa documental é bem semelhante com a bibliográfica (GIL, 2002).

3. Desenvolvimento

3.1 A Lei geral de proteção de dados: o marco regulatório da proteção dos dados pessoais no Brasil

A Lei 13.709/2018 conhecida como Lei Geral de Proteção de Dados (LGPD), foi criada para dispor sobre o tratamento de dados pessoais, em diferentes níveis, incluindo os meios digitais, sendo por pessoa física ou jurídica, protegendo assim, os direitos a privacidade individual e o livre desenvolvimento da personalidade (BRASIL, 2018).

Com esse objetivo, essa lei não visa apenas garantir a privacidade e a proteção de dados pessoais, mas também visa garantir a lealdade da concorrência econômica nos meios digitais, sendo aplicável a qualquer empresa de qualquer segmento, sem distinção entre elas, e com isso a LGPD delimita a proteção a quaisquer dados pessoais, sensíveis e anonimizados, definindo procedimentos de atuação na esfera comercial.

O Brasil sempre contou com algum método que procurasse proteger os dados do consumidor, baseando-se no código de defesa do consumidor, ou mesmo com leis mais específicas, como foi o caso da criação da lei Carolina Dieckmann, que prevê somente sobre a invasão de dispositivos.

A chegada da General Data Protection Regulation (GDPR) na comunidade europeia, em maio de 2018, mostrou que o vazamento de dados pessoais era um grave problema a ser tratado, e o poder público brasileiro viu nessa questão a necessidade de criar uma legislação interna, tanto para proteger o povo brasileiro quanto para conseguir entrar no seleto grupo de países que tem uma lei de proteção de dados regulamentada, utilizando isso como uma estratégia para a entrada na organização para Cooperação e Desenvolvimento Econômico (SOCIAL MINER, 2020).

As principais regulamentações da GDPR, além da expansão do conceito de dados pessoais, são:

Criação de Órgãos Controladores Locais nos países membros da Comunidade Europeia com o propósito de receber e investigar denúncias e reclamações sobre a adoção do GDPR. É necessário comunicar aos Órgãos Controladores Locais quaisquer violações que porventura tenham relações a dados pessoais, no prazo máximo de 72 horas. Caso a violação represente risco ao indivíduo, o qual os dados foram violados, este deverá ser comunicado.

Cada empresa/organização deverá nomear um representante responsável por gerir os dados pessoais e por implementar medidas técnicas e organizacionais adequadas para garantir que os dados pessoais sob poder da empresa correspondem com as normas da GDPR. Esse representante pode ser um indivíduo, um departamento ou até mesmo outra empresa externa.

Estabelecimento de diversos direitos aos cidadãos, como: o direito de ter seus dados excluídos pela organização quando solicitado; direito de não permitir que seus dados pessoais sejam utilizados em determinadas situações como em campanhas de "marketing"; direito de retificar seus dados, solicitando e indicando a correção de dados pessoais incompletos; direito de solicitar a transferência dos seus dados de uma organização para outra (portabilidade) sem burocracia; direito de pedir informações a respeito do processamento e armazenamento dos seus dados; e, por fim, direito à privacidade dos dados das crianças, sendo que todo e qualquer armazenamento de dados pessoais de menores de 13 anos precisam ter o consentimento dos responsáveis.

Vale a pena reiterar que toda organização que atua na Europa com coleta ou

tratamento de dados precisou promover adequações para atender essa Regulação. Nesse contexto, estão, inclusive, corporações como Amazon, Google, Facebook e Adobe com atividades na Europa.

A lei criada no Brasil que entrou em vigor em agosto de 2020, foi baseada na GDPR da União Europeia, que entrou em vigor em maio de 2018, o GDPR aplica-se a dados pessoais que "qualquer informação relacionada a uma pessoa física identificada ou identificável ('titular dos dados'); uma pessoa singular identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador on-line ou um ou mais fatores específicos para a identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.

Com essa nova lei, o Brasil também resolve questões comerciais que envolve países onde já existe a lei de proteção de dados, pois, muitas parcerias comerciais internacionais não podem ser feitas em relação a não conformidade do Brasil na questão de proteção de dados.

Os dados pessoais são conceituados a fim de delinear o escopo da aplicação da lei, criando regramento de toda informação relacionada ao indivíduo, que possa identificá-lo ou qualificá-lo, segundo o artigo 5.º, inciso I, da 13.709/2018 (BRASIL, 2018).

O artigo 5°, inciso II define que os dados pessoais merecem uma atenção especial, compostos por origem racial, religião, opinião sobre política, orientação sexual, filiação sindical, origem étnica (BRASIL, 2018).

Com isso, a lei esclarece que na utilização de dados sensíveis, fica proibido o processamento de dados de esfera individual sobre orientação sexual, a raça e etnia, a religião, a opinião política, os dados genéticos, os dados biométricos, bem como os dados relativos à saúde, exclusos casos que tenha o consentimento prévio do titular dos mesmos.

Quanto aos dados anonimizados, a legislação trata como dados relativos a um indivíduo não identificado, considerando assim o seu tratamento como meios técnicos razoáveis, conforme o artigo 5.º, inciso III da 13.709/2018 (BRASIL, 2018).

Alguns autores brasileiros procuram diferenciar dados de informações, Doneda (2014) ensina que dado é uma pré informação, apresentado de forma primitiva e abstrata como uma potencial informação, neste sentido a informação já passa a ser algo pleno, além do abstrato que se relaciona diretamente com a privacidade seja qual for sua difusão de informação.

3.2 A LGPD e a Privacy By Design nos termos de uso e política de privacidade

A Privacy By Design (PbD) é uma ferramenta que visa incorporar a privacidade ao “design” de sistemas ou produtos diretamente ao início de seu desenvolvimento e durante todo o seu ciclo de vida, incluindo o uso do sistema, foi desenvolvida pela Dra. Ann Cavoukian (Comissária de Informação e Privacidade de Ontário, Canadá) em meados dos anos 90, quando ela documentou os 7 Princípios Fundamentais (FOU). A Privacidade desde a concepção é baseada em 7 "princípios fundamentais":

1. Proativo, e não reativo; preventivo, e não corretivo: de modo a evitar incidentes de violação à privacidade antes que eles ocorram;

2. Privacidade como configuração padrão: as configurações padrão de determinado sistema deve ser ajustadas desde o início para preservar a privacidade do usuário;

3. Privacidade incorporada ao design: incluindo a arquitetura e modelos de negócio;

4. Funcionalidade total - soma positiva, não soma zero;

5. Segurança de ponta a ponta: proteção completa incorporada ao ciclo de vida da informação;

6. Visibilidade e transparência - mantê-lo aberto;

7. Respeito pela privacidade do usuário: mantê-lo centrado nos interesses do usuário (CAVOUKIAN, 2011).

O objetivo é proteger os dados pessoais em todas as fases do seu ciclo de vida, coleta, processamento, divulgação, armazenamento e descarte. A estrutura PbD pode ser aplicada não apenas em TI, mas também em práticas de negócios e em infraestrutura de rede, produto ou serviços, colocando a proteção da privacidade no escopo da estrutura, demonstrando também seus valores e conduta ética.

Privacidade e confidencialidade estão entre as metas básicas de segurança em qualquer Sistema de Tecnologia (TI). Essas metas de segurança geralmente são mal interpretadas e tomadas para significar o outro, mas são objetivos distintos que não devem ser confundidos.

A confidencialidade concentra-se na não divulgação de dados a pessoas não autorizadas ou entidades, enquanto a privacidade garante que haja controle sobre como os dados pessoais são coletados, armazenados e divulgados.

A Lei Geral de Proteção de Dados prevê em seu artigo 46, § 2.º, que os agentes de tratamento devem adotar medidas de segurança técnicas e administrativas desde a concepção, ou seja, refere-se à implantação da metodologia Privacy *By Design* durante o processo de negociação.

Atualmente os contratos por meios digitais são providos de um campo de aceite que fica localizado no final de todas as cláusulas, onde só com esse aceite o usuário tenha acesso à plataforma, existindo também cláusulas essenciais e mais importantes destacadas por letras maiúsculas e cores diferenciadas, caso se tenha modificações, possui a possibilidade do usuário ser informado através da plataforma, através de vários canais de comunicação, como os chats, por exemplo.

Novas empresas de tecnologia, como a *Uber* e o *Ebay*, elaboram seus termos de política e privacidade em um formato onde se proporciona uma melhor organização de informações aos usuários. Verifica-se que a *Uber*, empresa multinacional americana destinada ao fornecimento de serviços de transportes, divide sua Política de Privacidade em “introdução”, “visão geral”, “coletas e usos de dados”, “opções e transparência” “atualizações deste aviso”, de modo que o usuário pode optar por acessá-los separadamente (UBER TECNOLOGIA LTDA, 2019).

Nesse âmbito, a coleta de dados na plataforma da empresa passa a ser um indicador de informações que levará a empresa a criar um perfil de seu usuário, fazendo várias categorias de verificação, como, por exemplo verificações de segurança (UBER TECNOLOGIA LTDA, 2019). Dessa maneira, cada empresa utiliza-se dos dados forne-

cidos pelos seus usuários de uma maneira diferente, fazendo um delineamento necessário para cada tipo de utilização ou prestação de serviço.

Existem diversas outras empresas que seguem a mesma linha de tratamento de dados de seus usuários, como o Mercado Livre, *OLX*, 99 Pop, *WebMotors*, Google, YouTube entre outras, fazendo assim um tratamento geral de dados fornecidos pelos seus usuários de modo a lhes proporcionarem uma experiência que atendam suas expectativas e obedeçam a legislação vigente.

Na Figura 1, demonstra-se a Política de Privacidade do Mercado Livre

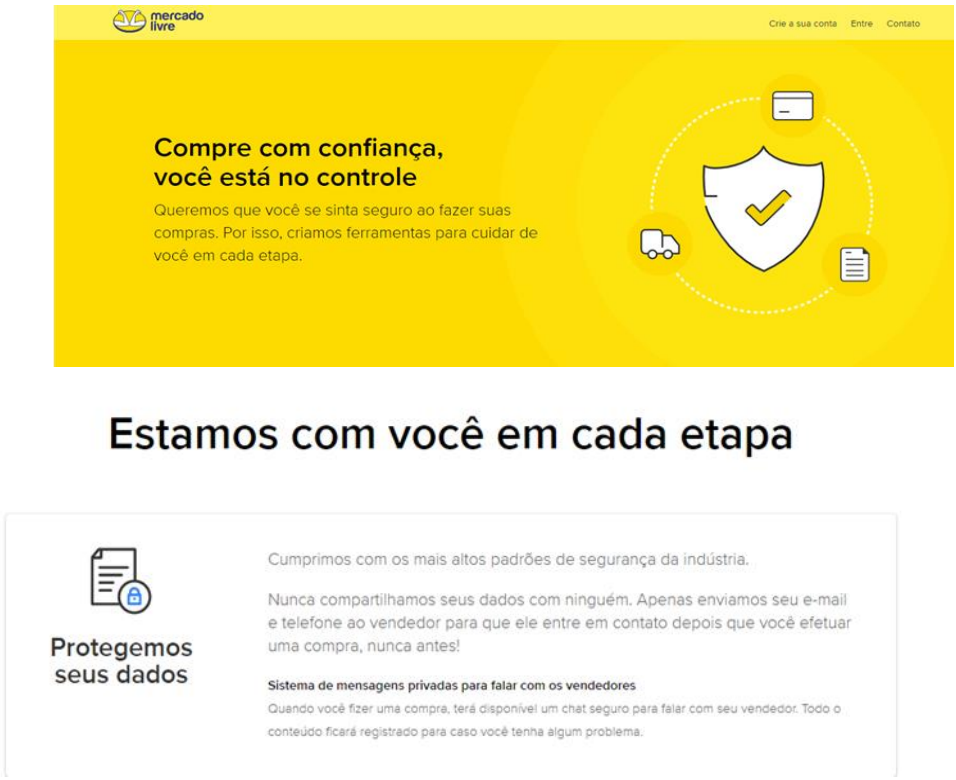

Figura 1. Fonte: Site do Mercado Livre, 2021

Diante deste exemplo, pode-se entender como as empresas devem se adequar e garantir a segurança de dados dos seus clientes, parceiros e fornecedores. Desta maneira, os usuários que preencherem seus dados sensíveis nos contratos, pedidos de compras ou cadastros diversos terão seus dados mantidos em segurança pela empresa responsável. Estes dados serão tratados pelos encarregados, os controladores, os operadores e agentes de tratamento de dados, que as empresas obrigatoriamente terão de contratar especificamente para o tratamento destas informações no setor de Tecnologia de Informação/ Tratamento dos Dados. Quando estes dados forem tratados irregularmente ou houver vazamentos as empresas poderão ser responsabilizadas cível e criminalmente, além de pagamento de multas aplicadas em até R$ 50 milhões pela Autoridade Nacional de Proteção de Dados (ANPD), além do risco de eliminação, bloqueio e suspensão das atividades de coleta das informações.

3.3 Tratamentos irregulares ou vazamento de Dados, a questão da responsabilidade empresarial conforme a LGPD

Diante deste cenário, as pessoas passaram a se ver de frente a novos riscos envolvendo seus dados e informações pessoais, criando assim uma nova sociedade de risco, Andrade; Acioli (2013, p. 107) expõem que:

> Tais riscos, além de possuírem o caráter global, tendo em vista que já não mais respeitam fronteiras territoriais ou sociais, são responsáveis por gerar situações de perigo ante o uso desmesurado das novas tecnologias capazes de atingir a própria noção de personalidade, bem como por causar novas situações de desigualdade social, constituindo em novos perigos decorrentes da modernização pelo desenvolvimento tecnológico.

Com isso, verifica-se que a sociedade de risco enfrenta constantemente o problema de vazamento de dados, dispostos as novas tecnologias, interferindo assim na esfera individual, lhes trazendo reflexos negativos. Desta forma, se estabelece que a LGPD surge para esclarecer dúvidas contidas nos contratos firmados por meio digital, redigindo assim a responsabilidade e deveres das empresas, principalmente na questão do tratamento de dados pessoais.

Com a legislação específica, novos meandros foram concebidos aos casos relativos ao vazamento de dados pessoais e demais tratamentos irregulares. Dessa forma, verifica-se que o legislador atribuiu uma seção própria para a responsabilidade e o ressarcimento dos danos e, em seu artigo 42, determinou a responsabilidade do controlador ou o operador que, em razão do tratamento de dados pessoais, causarem danos em violação à lei (BRASIL, 2018).

Para se constatar a violação da LGPD, o legislador tem que se atentar a vários fatores, pois sua violação não é nada simples de ser observada, sendo que as hipóteses onde o tratamento de dados será considerado irregular:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I – o modo pelo qual é realizado; II – o resultado e os riscos que razoavelmente dele se esperam; III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano (BRASIL, 2018).

Por se tratar de uma relação consumerista, isto é, em síntese, entre o fornecedor de serviços e o consumidor (titular dos dados), torna-se necessário observar o Código de Defesa do Consumidor. No artigo 14 do mesmo diploma, há a denominada responsabilidade pelo fato do serviço. São hipóteses onde o fornecedor será responsabilizado objetivamente, isto é, independente da análise de culpa, pelos danos causados por defeitos na prestação de serviço (BRASIL, 1990).

Além disso, o §1º do artigo 14 conceitua o serviço defeituoso, isto é, aquele que não fornece a segurança que o consumidor espera, quanto ao modo de fornecimento, aos resultados, riscos e considerando-se a época em que foi fornecido (BRASIL, 1990). Constata-se, portanto, que há significativa semelhança com o que a nova legislação prevê no que diz respeito aos tratamentos de dados pessoais irregulares.

Noutro giro, cabe analisar o que a LGPD descreve como "técnicas de tratamentos de dados pessoais disponíveis à época em que foi realizado", indicadas no inciso III do artigo 44 da lei, bem como expressamente mencionadas no artigo 46 da LGPD. Sob esse cenário, Corrêa (2019) entende que a verificação em concreto das "técnicas que eram disponíveis à época onde o tratamento de dados foi realizado", exige um posicionamento específico dos julgadores, dotado de certa profundidade técnica. Esta profundidade, para fins de se apurar a responsabilidade dos agentes de tratamento, demandaria a utilização de prova pericial quanto ao vazamento de dados, nos moldes do artigo 474 do Código de Processo Civil brasileiro de 2015 – CPC (BRASIL, 2015).

Portanto, somente com a perícia finalizada é que seria possível comprovar o ato ilícito, com o nexo causal e o dano realizado ao titular de dados, que compõem os elementos da responsabilidade civil objetiva.

Diante do apresentado, fica esclarecido que a LGPD não busca apenas incentivar a proteção de dados das pessoas, mas também procura promover e proteger os dados em sua integralidade, e equilibrar uma relação justa entre empresas e consumidores, para que não se tenha abusos e excessos por parte de empresas e prestações de serviços.

3.4 Os Dados Pessoais e sua utilização como estratégias de negócios

A Sociedade da Informação propiciou a criação de empresas com características completamente diferentes daquelas do passado, como as organizações digitais, entendendo organização digital não somente como aquelas que têm extensão virtual e são físicas, mas também aquelas que existem só virtualmente, sem ter uma loja física e só vendem seus produtos via *internet*, como a *Amazon* (PINHEIRO, 2016).

A Sociedade da Informação, sem dúvida nenhuma, revolucionou os mercados e os produtos. Os custos baixaram devidos à globalização, as mercadorias são fabricadas em escala que atendam ao apelo de consumo, não por necessidade, mas por *status*, em especial. O consumo interfere até mesmo nas relações sociais e é, por muitos, visto como a solução de diversos problemas (CAVALCANTI, 2017).

Na concepção de Lisboa, a modernidade trouxe um novo padrão de economia, a "economia do descartável". A sociedade atual é consumista, e isso implica em dizer que a satisfação do cliente não tem relação com o produto em si e sua funcionalidade, mas sim com sua satisfação pessoal em adquiri-lo (LISBOA, 2006).

Os atos de consumo - incluindo muitos atos realizados em momentos anteriores ao consumo em si - proporcionam, neste panorama, a compilação de abundante informação sobre o consumidor, o que veio a modificar o perfil do fluxo informacional entre fornecedor e consumidor: agora, é possível ao fornecedor saber detalhes não somente sobre grupos de consumidores, porém sobre o consumidor individualmente considerado, o que abre a possibilidade de sua abordagem de forma pretensamente individualizada. O consumidor, enfim, aos olhos da atividade de marketing, não é mais somente o destinatário de informações, porém tornou-se fonte de informações que vão determinar a forma como ele poderá ser abordado e tratado (DONEDA, 2011).

Para Antonialli (2017), muitos produtos e serviços ofertados na *Internet* são gratuitos ou oferecem, no mínimo, versões gratuitas, a seguir: redes sociais, *webmails*, plataformas de compartilhamento de imagens e vídeos e diversos outros aplicativos com várias funcionalidades, como jogos e agregadores de informações.

A grande maioria dos modelos de negócio que viabilizam esse oferecimento gratuito de produtos e serviços está fundada na publicidade digital. Embora a lógica seja fundamentalmente a mesma daquela que financia a produção de conteúdo para parte da imprensa escrita e televisionada, qual seja a venda de espaços publicitários para anunciantes, o ambiente digital sofisticou muito a possibilidade de monetização desses espaços, fazendo que eles sejam também, muitas vezes, menos transparentes. Isso porque a partir da coleta e tratamento de dados pessoais é possível segmentar usuários por grupos de interesse específicos e, portanto, direcionar os anúncios de forma mais eficiente (ANTONIALLI, 2017).

Diante dessa perspectiva, o número de usuários é essencial para a empresa que divulga anúncios. Também é importante a coleta de dados desses usuários, visto que quanto maior for a coleta, maior o nível de precisão com o qual a empresa determinará a importância dos anúncios que serão exibidos e, em consequência, maior o valor a ser cobrado por cada exibição (ANDERSON, 2009).

Novas fontes de dados gerados por meios sociais e pelo crescimento da telefonia móvel e sistemas digitais diversificados de captação da informação e imagens, possuem potencial de modificar por completo o processo tradicional de geração de valor de uma companhia. A boa aglutinação destes dados, em uma base digital adequada, pode gerar conhecimentos adicionais sobre o interesse, as paixões as afiliações, redes e relações do usuário, além de elementos de fidelização de tal ordem que se otimize ao infinito o processo de captação e prospecção de clientela. Por esse motivo, a coleta de dados pessoais é uma prática recorrente e silenciosa entre as empresas da área virtual da *internet* (ANTONIALLI, 2017).

Muitas vezes sem perceber, o usuário tem seus hábitos e preferências de navegação monitorados por meio da utilização de diversos mecanismos tecnológicos diferentes de coleta de dados, como os cookies. Os cookies são pequenos arquivos que podem ser enviados durante a comunicação estabelecida entre o dispositivo do usuário e o servidor do site que está sendo visitado. Esses arquivos nada mais são do que identificadores, que tornam possível reconhecer o dispositivo em visitas futuras e armazenar informações sobre suas preferências, por exemplo. É graças aos cookies que itens podem ser adicionados e mantidos em “carrinhos de compra” virtuais ou que preferências de exibição de páginas podem ser configuradas para visitas futuras (ANTONIALLI, 2017).

Quando as empresas têm acesso aos dados dos usuários, são criados bancos de dados com informações pessoais, tais como palavras buscadas, *sites* visitados, compras realizadas e até lugares visitados. Somam-se a esses fatos os arquivos que ficam armazenados nos servidores das empresas. A divisão dos usuários com base nesses dados e inferências, gerou o desenvolvimento de sistemas automatizados complexos de alocação e exibição de anúncios, cujo funcionamento depende de mecanismos de “leilões”.

Inicialmente, esses mecanismos foram desenvolvidos para os anúncios oferecidos em buscadores, como *Yahoo e Google*. Basicamente, cada anunciante poderia propor um valor (lance) para a exibição de um determinado anúncio associado a uma palavra-chave (termo). A cada busca realizada pelo referido termo, o buscador considerava o lance do anunciante em comparação com os lances de outros anunciantes associados à mesma palavra-chave, como em um sistema tradicional de leilão. Os resultados de busca patrocinados (anúncios) eram então exibidos em ordem decrescente, ficando, no topo, o anúncio associado ao lance de maior valor e assim sucessivamente. Os anunciantes cujos anúncios recebessem cliques pagavam os valores com os quais haviam se comprometido (lance) (ANTONIALLI, 2017).

No decorrer do tempo, mecanismos semelhantes foram utilizados para definir quais anúncios seriam exibidos para cada usuário. Em outras palavras, em quase todos os sites há um sistema automatizado de leilões, administrado por agências e redes de anunciantes, intermediários que promovem a ligação entre os anunciantes, as plataformas e o usuário, conforme definem quais anúncios serão exibidos para quais grupos de usuários (ANTONIALLI, 2017).

Para Doneda (2011), a maioria dos dados obtidos do consumidor não são obtidos por sua livre expressão, mas sim em informações articuladas a seu comportamento cotidiano, tal como, navegando na *internet* ou em situações de consumo. Tais informações comportamentais são fornecidas sem que o consumidor perceba, sendo que isso não ocorre com a mensagem publicitária do fornecedor, criteriosamente selecionada de acordo com o perfil do consumidor.

A publicidade comportamental faz uso de informações sobre o comportamento do indivíduo para que se especifique qual abordagem será mais adequada. Atualmente, a *Internet* é uma das fontes de dados mais visadas para a obtenção de dados que estabeleçam o "perfil" de um consumidor tendo como ponto de partida seu comportamento por intermédio do seu histórico de navegação (DONEDA, 2011).

É fundamental notar, no entanto, que a compilação de perfis de comportamento tem a publicidade comportamental como apenas uma de seus potenciais finalidades. Hoje, a forte dinâmica deste mercado o coloca em posição de destaque, porém qualquer atividade que possa ter a ganhar com um conhecimento mais apurado de uma pessoa ou uma possibilidade de antever suas opções futuras tem muito a ganhar com a existência destes perfis.

Desta forma, somente para fornecermos alguns exemplos, tanto campanhas eleitorais como o recrutamento de recursos humanos, a compilação de históricos clínicos ou a precificação de seguros, além de tantos outros, podem apresentar um interesse potencial nestes perfis, levando a situações de relativização da liberdade de escolha e mesmo de discriminação que, embora possam ultrapassar o alcance da relação de consumo, decorrem desta estrutura montada no âmago da publicidade para o consumidor. Não seria a primeira vez que o direito do consumidor se encontra na vanguarda da regulação de uma atividade cujos efeitos potenciais podem, a curto e médio prazo, ultrapassar largamente a alçada da proteção do consumidor, e este fato apenas ressalta a vocação deste ramo do direito para ser também um laboratório de soluções e técnicas jurídicas que possam se demonstrar viáveis e, ao fim, transferidas e traduzidas para outras situações (DONEDA, 2011). Segundo Bioni (2014), o mercado informacional é uma realidade. Os dados pessoais impulsionam a economia e constitui-se em uma de suas mais importantes ferramentas. Sendo assim, a agenda da privacidade está economizada como nunca antes visto na história.

4 Considerações finais

O Brasil é um dos países onde se mais tem acesso à *"internet"*, em uma pesquisa promovida pelo Comitê Gestor da Internet do Brasil demonstrou que em 2020, o país chegou a 152 milhões de usuários, visualizando também que 81% da população com mais de 10 anos tem internet em casa. Diante disso o Brasil é o país onde sua nação tem os seus dados mais vulneráveis se comparados a outros países.

Pode-se observar que os meios eletrônicos de consumo estão cada vez mais presente na vida das pessoas, contudo, as leis impostas até então se baseavam no código de defesa do consumidor, onde o comércio eletrônico ainda não era uma prática usual. Com o advento da informática e o comércio eletrônico, os dados pessoais passaram a ser utilizados como um dos meios de atrair o consumidor, que pode efetuar uma compra de forma impulsiva ou induzida com base em sua idade, gênero ou outras informações pessoais, portanto, a criação de ferramentas que norteiam esse uso trazem benefícios à população.

Com a criação da Lei Geral de Proteção de Dados, as empresas estarão obrigadas a fazer um tratamento diferenciado e mais cuidadoso com os dados pessoais de seus clientes, e no demais a lei criou regras entre clientes e empresas no mercado virtual, coibindo e fiscalizando os excessos e abusos que vira a ser praticados, regulando essa nova modalidade em amplo crescimento.

Empresas e órgãos públicos poderão ser punidos pelo uso indevido dos dados pessoais de consumidores e cidadãos, incluindo vazamentos de dados pelas sanções serão aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD). As exigências da LGPD valem tanto para as lojas físicas quanto para virtuais, situadas no país ou no exterior que ofereçam serviços para pessoas no Brasil. Desta forma, as empresas deverão se adaptar a esta nova realidade através da contratação de profissionais: (DPO Data Protection Officer - encarregado, os controladores, os operadores e agentes de tratamento de dados, para tratar dos dados sensíveis de seus clientes através de ferramentas adequadas de T.I para garantir que haja o cumprimento da legislação vigente.

A Lei Geral de proteção de dados é uma lei que norteia o uso e armazenamento de dados pessoais, trazendo mais segurança aos usuários para qualquer ramo de atividade. Para tanto a adoção de técnicas e ferramentas como PbD permitem maior segurança e confiabilidade dos sistemas utilizados pelas empresas. É importante ressaltar que empresas multinacionais como Google e Microsoft não perceberam impacto com as novas exigências, tendo em vista que suas ações seguem regulamentações internacionais que já preveem a segurança dos dados dos seus usuários.

Referências

ANDERSON, C. (2009). FREE: The Future of a Radical Price, New York: Hyperion.

ANDRADE, F.S. ACIOLI, C.G. (2013). A inclusão digital no Brasil e a responsabilidade civil estatal por omissão. Revista de Direitos e Garantias Fundamentais, 14 (2).

ANTONIALLI, D. M. (2017). Representante do Internetlab questiona bloqueio de aplicativos por descumprimento de ordem judicia. Notícias STF, Brasília.

BIONI, B. R. (2014). A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço. In: Aires José Rover, José Renato Gaziero Cella, Fernando Galindo Ayuda. (Org.). Direito e novas

tecnologias: XXIII encontro nacional do CONPEDI. 1ed. Florianópolis: Conpediv.

BRASIL. Constituição da República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 nov. 2021.

BRASIL. Lei 13. 709, de 14 de agosto de 2018. Diário Oficial da República Federativa do Brasil. Brasília, DF: 14 ago. 2018.

CAVOUKIAN, A. (2011). **Information & Privacy: 7 foundational principles**. Architecture Board. Disponível em: https://www.iab.org/.Acesso em: 01 dez.2021.

CAVALCANTI, A. E. L.W. (2007). O direito na sociedade da Informação. 1ªed. São Paulo: Atlas, v. 01, p. 143-158.

CORRÊA, L. (2019). É importante não perder o foco da segurança jurídica no âmbito da LGPD. In: Revista Consultor Jurídico, 03 de março de 2019. Disponível em: https://www.conjur.com.br/2019-mar-03/leonardo-correa-seguranca-juridica-ambito-lgpd. Acesso em: 17 nov. 2021.

DONEDA, D. (2014). O direito fundamental à proteção de dados pessoais. Direito Privado e Internet: atualizado pela Lei nº 12.965/2014: Marco Civil da Internet no Brasil. São Paulo: Atlas, p. 61- 78.

GIL, A. C. (2012). Métodos e Técnicas de Pesquisa Social. 6 ed. São Paulo: Atlas.

GONÇALVES, C. R. (2012). Direito Civil Brasileiro: Resp. Civil. 7. ed. São Paulo.

LISBOA, R.S. (2006). Direito na Sociedade da Informação. RT, São Paulo, v. 847.

PINHEIRO, P.P. (2016). Direito Digital. São Paulo: Saraiva.

SOCIAL MINER. (2021). Tudo que sua empresa precisa saber sobre a LGPD. Disponível em: http://blog.socialminer.com/people-marketing/privacidade-de-dados-e-tudo-sobre-a-lgpd/ Acesso em: 17 nov. 2021.

UBER TECNOLOGIA LTDA. (2019). Aviso de Privacidade – Última atualização: 12 de novembro de 2019. Disponível em:uber.us.com. Acesso em: 17 nov. 2021.

ZUBOFF, S. (2019). The age of the surveillance capitalism. London: Profile Books.