PRIVACIDADE E PROTEÇÃO DE DADOS NA ERA DO BIG DATA
PRIVACY AND PROTECTION IN THE BIG DATA ERA

CARLOS EDUARDO LESSA SANTOS [*]
FELIPE FREIRE DE CARVALHO [**]

Resumo

Vivemos uma nova era, um novo contexto, com grande volume de dados e informações, denominado Big Data. Os dados se apresentam como matéria-prima da informação, uma enorme fonte de valor econômico e social. Avanços na mineração de dados e análises, em convergência com aumento do poder computacional de processamento e armazenamento, aumentou expressivamente as informações disponíveis para entidades públicas e privadas. Porém, os usuários podem não ter conhecimento das aplicações do Big Data e ao mesmo tempo, podem ter a sensação de invasão de privacidade. Este trabalho, visa proporcionar um debate sobre o alcance da Lei Geral de Proteção de Dados Pessoais (LGPD), sobre os grandes conjuntos de dados que precisam ser processados e armazenados; apontando a necessidade de discutir o Big Data, com ênfase nas políticas de acesso à informação e privacidade.

Palavras-chave: Big Data. Privacidade. LGPD. GDPR. Segurança da Informação. Análise de Dados.

Abstract

We live in a new age, a new context, with huge amounts of data and information, called Big Data. Data is presented as the raw material of information, a huge source of economic and social value. Advances in data mining and analytics, in convergence with increased computational processing and storage power, have significantly increased the information availability to public and private entities. However, users may be unaware of Big Data applications and the risks of invasion of their privacy. This paper aims to provide a debate about the Brazilian

---

Trabalho de conclusão de curso apresentado ao curso de Bacharelado em Sistemas de Informação da Universidade Federal Fluminense como requisito parcial para conclusão do curso.
[*]Graduando do Curso de Sistemas de Informação-UFF; c.eduardo.lessa@gmail.com
[**]Graduando do Curso de Sistemas de Informação-UFF; ffdcarvalho@hotmail.com

Personal Data General Law, called Lei Geral de Proteção de Dados Pessoais, pointing out to the need of discussing Big Data, with an emphasis on information access and privacy policies.

Keywords: Big Data. Privacy. LGPD. GDPR. Information Security. Data Analysis.

Aprovado em: 10/12/2019 Versão Final em: 17/12/2019

1 **INTRODUÇÃO**

O novo modelo comportamental dos indivíduos no século XXI, associado à intrínseca utilização da Internet, tem permitido e impulsionado que entidades públicas ou privadas operem cada vez mais no âmbito virtual, utilizando-se da tecnologia da informação para estabelecer comunicação e promover transações entre diversos grupos de stakeholders. De acordo com Manuel Castells, a sociedade contemporânea se depara com uma revolução tecnológica, cuja essência está pautada nos sistemas de informação, de processamento e de comunicação (CASTELLS, 1999).

Dito isso, os fatores que motivam o comportamento dos usuários de sistemas online têm ganhado relevância, uma vez que permite que as empresas possam identificar necessidades e ações de negócio concreto, objetivando otimizar a oferta de produtos e/ou serviços, promovendo uma melhor experiência para seu usuário. Desta forma, constatamos que o avanço no desenvolvimento de tecnologias de mineração e armazenamento de dados, proporciona identificar padrões implícitos de comportamentos dos indivíduos.

A quantidade de dados gerados por sites, redes sociais, sensores, aplicativos e muitas outras corporações públicas ou privadas, está aumentando drasticamente, mais de 2,5 quintilhões de bytes de dados são gerados em todo o mundo todos os dias (DOMO, 2019). A enorme quantidade de dados gerados, sendo grande parte dados pessoais, a partir de fontes diferentes e em formatos variados, aliados a formas inovadoras e econômicas de processamento de informações que permitem uma melhor tomada de decisão, é referido como Big Data (DOUG LANEY, 2001).

Este artigo aborda as questões legais decorrentes do debate sobre Big Data. Sugere que os princípios práticos da informação justa (Fair Information Practice Principles - FIPPs) devem ser vistos como um conjunto de engrenagens a serem ajustadas de acordo com as condições

comerciais e tecnológicas (HOMELAND SECURITY, 2008). De fato, a engenhosidade dos FIPPs é manifestada em sua flexibilidade, que os tornou resilientes a mudanças importantes. Dentro do contexto de Big Data, isso significa atenuar os requisitos de minimização e consentimento de dados, enfatizando transparência, acesso e precisão. A mudança visa capacitar indivíduos sobre a coleta de informações, que tradicionalmente giravam em torno de políticas de privacidade corporativa raramente lidas, muito menos compreendidas, que permitem aos envolvidos se beneficiarem de informações já coletadas. Além disso, essa exposição impedirá a existência de bancos de dados 'secretos' e alavancar a pressão social para restringir usos inaceitáveis.

A revista The Economist (CYBERWAR, 2010) retrata o conflito de escolha entre os benefícios econômicos trazidos pela utilização do Big Data e os riscos à privacidade. A Comissão Europeia, no ano de 2012 (COMISSÃO EUROPEIA, 2012), alerta sobre o novo modelo econômico e comportamental adotado na Internet, onde em relatos considera as normas de privacidade adotadas em sites altamente arriscadas, ainda que houvesse respaldo legal no momento. Tal observação motivou a adequação da legislação Europeia a essa nova realidade. A percepção da Comissão Europeia, além dos aspectos referidos ao risco severo da privacidade individual, com a unificação e correlação de dados de usuários entre diferentes serviços é a preocupação relativa ao desconhecimento dos conceitos básicos de Big Data pela sociedade (MELANIE VOIN, 2015).

No entanto, a adequação legislativa realizada pela União Europeia, apresenta fragilidades quanto a sua aplicabilidade em Big Data, correlação de dados e inferências. Os indivíduos obtêm pouco controle sobre como seus dados são utilizados para gerar conteúdos sobre eles mesmos, realizando estudos de predileção. Em relação a demais dados pessoais, as inferências atuam principalmente sobre a sua classe econômica e modelo de consumo. No Regulamento Geral de Proteção de Dados (GDPR), os direitos dos titulares de dados de conhecer (Art. 13-15), retificar (Art. 16), excluir (Art. 17), ou posse (Art. 20) são significativamente reduzidos, quando para realização de inferências (EUROPA, 2018).

Em contexto nacional, o Marco Civil da internet surgiu há 10 anos e trata dos princípios, garantias, direitos e deveres para quem utiliza a rede. A Lei Geral de Proteção de Dados (LGPD), que entrará em vigor em agosto de 2020 (BRASIL, 2018), estabelece a normativa para

tratamento de dados, que pode ser interpretado como qualquer procedimento que envolva a utilização de dados pessoais.

O objetivo deste trabalho é analisar a nova lei LGPD, considerando se as suas diretrizes conseguem ou não nortear as ações de segurança da informação, promovendo a efetiva proteção de dados pessoais no contexto de Big Data. É neste sentido que se encontram os problemas a serem estudados. Para tanto, dividiu-se o presente trabalho em quatro seções. Na primeira seção analisou-se os conceitos de Big Data. Na segunda seção, examinou-se qual a fundamentação do tratamento de dados pessoais. A terceira seção trata sobre o Direito à privacidade na era digital. Por fim na quarta seção é apresentado um cenário de aplicação de estudo. Fez-se uso da pesquisa bibliográfica exploratória, através de livros e artigos, compreendendo legislações com enfoque em proteção e privacidade de dados e suas aplicações no modelo de grandes massas de dados.

2 **BIG DATA**

Ao longo dos anos de 2001 até os dias atuais o Big Data ganhou diversos conceitos de alguns autores e instituições. A TechAmerica Foundation define desse modo:

> Big Data é um termo que descreve grandes volumes de dados de alta velocidade, complexos e variáveis que requerem técnicas e tecnologias avançadas para permitir a captura, o armazenamento, a distribuição, o gerenciamento e a análise das informações (TECHAMERICA FOUNDATION, 2012).

Outra definição é a apresentada por Gunther:

> Big Data pode ser definido com base em grandes volumes de dados amplamente variados que são gerados, capturados e processados em alta velocidade. Como tal, esses dados são difíceis de processar usando as tecnologias existentes. Ao adotar tecnologias analíticas avançadas, as organizações podem usar Big Data para desenvolver insights, produtos e serviços inovadores (GÜNTHER, 2017).

Como é possível notar nas citações acima o volume de dados, velocidade de processamento e a variedade dos dados são apresentados como os alicerces do conceito de Big Data. Esses três principais pilares quando bem trabalhados podem gerar o tão esperado valor para os produtos e serviços das empresas ou governos.

2.1 **BENEFÍCIOS E APLICAÇÕES**

Agregar valor utilizando Big Data é mais do que simplesmente analisá-lo (o que é um outro benefício). É todo um processo de descoberta completo que exige analistas capacitados e bem qualificados além de usuários de negócios e executivos que são capazes de fazer as perguntas certas e reconhecer padrões, inferir dados e prever comportamentos. Big Data pode trazer respostas mais completas, nas mais diversas áreas melhorando a experiência entre cliente e empresas, a prevenção de fraudes, tornando a cadeia de fornecimento melhor conectada, promovendo o recrutamento e desenvolvimento de novos talentos para as empresas de forma aprimorada, pesquisas científicas dentre outras, porque tem mais informações. Obter respostas mais completas, se traduz em ter mais confiança nos dados, trazendo uma abordagem completamente diferente ao lidar com problemas.

O Big Data pode auxiliar as empresas e clientes na **tomada de decisões** uma vez que por meio da análise de grande volume de dados corporativos é possível chegar a insights valiosos a respeito das tendências e necessidades dos seus clientes, ajudando as empresas a tomarem decisões melhores de forma mais rápida. **Identificar padrões comportamentais** de seus clientes traçando assim perfis de forma a poder entregar ofertas de produtos e serviços personalizados e direcionados para os vários tipos de consumidores. Isto ajuda as empresas a mitigar as falhas na comunicação com seus clientes que a cada dia estão mais exigentes ao não oferecer ofertas genéricas. **Criação de estratégias de marketing** visto que os insights fornecidos pela análise dos dados ajudam a encontrar potenciais clientes e descobrir alterações em suas preferências. Dessa forma é possível criar estratégias de marketing melhores e mais lucrativas ao direcionar os investimentos para os segmentos corretos. **Acompanhamento da concorrência** entendendo e prevendo as novas demandas do mercado bem como as necessidades dos consumidores, a análise de grande volume de dados ajuda as empresas a saberem quais os próximos passos da concorrência ajudando na criação de caminhos diferentes

e mais eficientes. Assim, por exemplo é possível preparar promoções com produtos e serviços mais desejados estando na frente das empresas concorrentes (WESTCON, 2019).

Otimização dos processos internos visto que as empresas compreendem melhor o que estão fazendo de forma eficiente visando a identificar quais as falhas e gargalos há em seus respectivos processos. Elas conseguem visualizar as causas dos problemas mais recorrentes para tomar as medidas necessárias para modificar os procedimentos capazes de diminuir os possíveis problemas. **Relacionamento com o cliente** é outro importante ponto que se pode otimizar com o tratamento do grande volume de dados pois é possível detectar quais os desejos, insatisfações e as diversas necessidades de seus consumidores. **Melhoria da cibersegurança** pois com o aumento gradativo de ataques às redes corporativas é cada vez maior a necessidade das empresas buscarem novos métodos e mais eficientes de proteção. Com a análise dos dados é possível identificar prováveis ameaças ao monitorar vastos fluxos de informação detectando atividades suspeitas e comportamento estranhos de acessos de usuários a rede corporativa. **Gerenciamento de risco** ao oferecer informações mais aprimoradas sobre o tempo de produção e entrega de produtos aos clientes visualizando possíveis problemas na rotina produtiva permitindo que as empresas melhorem esse tempo evitando problemas internos e atrasos (WESTCON, 2019).

Investir em Big Data Analytics leva a empresa a lidar de forma otimizada e mais eficiente com seus processos aumentando sua receita com novos produtos e serviços personalizados. Com isso as empresas acabam atraindo novos clientes através do aprofundamento do conhecimento que possuem sobre os padrões de consumo do seu público. Tudo isso é capaz de proporcionar uma grande vantagem competitiva de mercado.

2.2 PREOCUPAÇÕES COM O ARMAZENAMENTO E TRATAMENTO DE DADOS

Big Data traz uma série de novas oportunidades que podem proporcionar vantagens competitivas ao mundo dos negócios, mas também há preocupações relevantes sobre seu uso. Seus efeitos podem ser positivos para algumas pessoas e negativos para outras. Há dois importantes pontos negativos do uso de Big Data: possíveis invasões de privacidade e a discriminação. Porém esses não são os únicos efeitos negativos possíveis. A perda de autonomia, descaracterização do indivíduo, classificação das pessoas ou grupos de pessoas de

forma desagradável, fornecimento unilateral de informação e o confronto com informações indesejadas são preocupações intrínsecas ao tratamento de dados (DANIEL MARTINS, 2019).

Uma boa medida para se classificar é a criação de perfis, denominado como desindividualização. Entretanto, isto é algo um tanto impreciso, pois existe um risco real de que as pessoas classificadas ao se criar o perfil sejam julgadas baseado nas características do grupo como um todo e não em seus próprios méritos e características pessoais. Perfis em grupo normalmente se originam de estatísticas. Assim os aspectos do grupo podem ser válidos para o grupo e para indivíduos membros desse grupo, mas não para os indivíduos em si. Podemos citar por exemplo, pessoas de determinada faixa etária que possuem menor ou maior probabilidade de se acidentar no trânsito e isto por si só causar uma alteração no valor do seguro de seus carros. Quando as pessoas são julgadas pelos critérios e aspectos do grupo, as quais não possuem como indivíduos, isso pode afetá-las negativamente. O perfil do grupo pode causar efeitos indesejados diretamente nos indivíduos pertencentes àquele grupo e pode ainda levar à sua estigmatização. Dividir em grupos pode prejudicar a harmonia social. Caso esses perfis tornem-se públicos, as pessoas podem começar a tratar os indivíduos de acordo com as características daquele grupo, desconsiderando o indivíduo em si (DANIEL MARTINS, 2019).

Mais um risco relacionado à criação de perfis é que ele pode levar a desarmonia de informações. Criando perfis, a posição do controlador de dados melhora em relação aos dados que possui à sua disposição, mas a posição de quem cede os dados continua a mesma. Isso ocorre quando o titular dos dados não possui o mínimo de conhecimento da criação do perfil dos quais seus dados estão sendo utilizados. A desarmonia de informação pode trazer uma desproporção de poder entre cidadãos e o governo e entre os consumidores e as empresas, causando um desequilíbrio entre as partes. Com relação a administração pública, a desarmonia de informação pode afetar a autonomia individual de cada cidadão. Se a mineração dos dados produzir informações que o Estado ou as empresas possam usar, então eles terão mais poder. O medo de ser monitorado, de ter seus dados capturado inapropriadamente e ser colocado em determinado perfil de grupo gera um efeito colateral indesejado em sociedades democráticas. Na relação entre consumidores e mercado, as desarmonias de informações podem levar por exemplo a preços discriminatórios como no caso do seguro de carro acima citado e a práticas econômicas desleais. Como ocorre muito hoje em dia, alguns serviços e produtos são oferecidos a determinados consumidores por estes se encaixarem ou não em determinados perfis. Também é possível ajustar preços de bens e serviços com base no perfil do indivíduo. Cobrar preços

diferentes baseados em aspectos específicos como sexo, preferência sexual e raça é uma violação da legislação brasileira anti-discriminação (DANIEL MARTINS, 2019).

Dividir e classificar pessoas é a atividade mais importante ao se criar perfis. Desse modo a discriminação é parte intrínseca dessa atividade visto que há situações nas quais esta prática é considerada ilegal e antiética. Isso acontece quando ao se definir o perfil do grupo isso é feito de forma indevida com finalidade diferente do inicial proposto no processamento de dados em relação aos aspectos de religião, gênero, etnia ou orientação sexual. Mesmo sem a intenção de julgar as pessoas com base em seus aspectos peculiares, há o risco de discriminação contra indivíduos específicos ou grupos (DANIEL MARTINS, 2019).

Outro risco associado ao Big Data é a imprecisão associada à criação de perfis, pois podem não ser fidedignos à realidade. Ocorrem problemas como falsos negativos e/ou falsos positivos. Pessoas são encaixadas dentro de determinados perfis os quais ela não deveria pertencer (falso positivo), e/ou pessoas que deveriam pertencer a um determinado perfil, mas por algum motivo são deixadas de fora (falso negativo). Uma das causas disso acontecer são por motivos de dados insuficientes que podem traçar de modo mais adequado o perfil do indivíduo. Isso leva ao problema quando se trata em decisões automatizadas sem intervenção humana. Por não haver um processo contraditório, não há um devido processo legal, pois ambos os lados não são ouvidos. Nesses casos o ônus da prova cabe ao titular dos dados sendo ele quem tem de provar que não deveria pertencer ao grupo colocado pelo Estado ou corporações (DANIEL MARTINS, 2019).

Ligado aos riscos de classificação das pessoas ou grupos de pessoas de forma desagradável e descaracterização do indivíduo, está o risco de se criar estereótipos onde um determinado perfil molda seus membros com base em categorias predeterminadas. Por exemplo cliente importante, indivíduo perigoso e profissional não urbano idoso. Um número finito de criação de perfis torna o processo mais eficiente, porém isso pode ocasionar que estes se tornem incapazes de refletir de forma precisa todos os aspectos de nossa personalidade. Apesar disso o perfil no qual cada um é encaixado se torna um estereótipo com base no qual ele será avaliado (DANIEL MARTINS, 2019).

Por fim, outro risco ligado à criação de perfis é o lado ruim humano onde pessoas que detém os dados de outras pessoas analisadas (membros do Estado, funcionários de corporações, hackers)

podem usá-los de forma abusiva. Isso piora quando um perfil pode ser associado com precisão a um indivíduo identificável. Logo um perfil antes particular que se torna público pode acarretar danos à reputação do indivíduo ou seus dados podem ser utilizados para fins nocivos (DANIEL MARTINS, 2019).

3 TRATAMENTO DE DADOS PESSOAIS

A evolução rápida das tecnologias de informação e comunicação, especialmente o uso intensivo da Internet, ilimitado no tempo e no espaço, levou ao crescimento do volume e da variedade de dados que podem ser combinados, aumentando o risco de re-identificação mesmo após a anonimização ou desidentificação de bases isoladas (MOONEY SJ, PEJAVER V, 2018). O reconhecimento da pouca efetividade de procedimentos de anonimização, desidentificação e do consentimento informado na proteção da privacidade têm cada vez mais valorizado a necessidade da implantação de mecanismos que permitam o maior controle sobre uso que se faz dos dados (MCGRAIL KM, GUTTERIDGE K, MEAGHER NL, 2015).

Desta forma torna-se ser necessária a utilização de mecanismos que possibilitem ao indivíduo obter conhecimento e controle sobre seus próprios dados que, no fundo, são expressão direta de sua própria personalidade (DONEDA, 2006). Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental.

3.1 PRINCÍPIOS PARA O TRATAMENTO DE DADOS PESSOAIS

No Brasil, a experiência política até 1988 e a nova Constituição Federal é o desencontro de um país com sua população. Quase dois séculos de ilegitimidade do poder, falta de efetividade das Constituições e violações da legalidade (LUIZ R. BARROSO, ANA PAULA DE BARCELOS, 2003). Os princípios sequer tinham força normativa, além de não possuírem vontade política que lhes desses aplicabilidade (DANIEL VIDOR, *2019*). Com a evolução do Direito, eles passaram a ser comandos com efetividade e juridicidade, que devem ser obedecidos por todos e que servem de alicerce para a aplicação imediata de outros direitos subjetivos. Sua importância tornou-se tal que sua violação é considerada a mais grave ilegalidade ou inconstitucionalidade. Nesse sentido, Celso Antônio Bandeira de Mello (MALHEIROS, 2000) afirma que:

> Violar um princípio é muito mais grave que transgredir uma norma qualquer. A desatenção ao princípio implica ofensa não apenas a um específico mandamento obrigatório, mas a todo o sistema de comandos. É a mais grave forma de ilegalidade ou inconstitucionalidade, conforme o escalão do princípio atingido (…).

Desta forma, a constituição acentua a força normativa dos princípios constitucionais, suplantando a doutrina positivista das normas programáticas (LUCIANO ROLIM, 2002). Neste contexto, são apresentados abaixo os princípios que a LGPD consagra e sua descrição. Os princípios estão positivados no art. 6º, caput e incisos de I a X (BRASIL, 2018).

A boa-fé presume que as pessoas ajam com boas intenções na realização de negócios jurídicos. Contrariá-lo geraria um ônus ao infrator. Como previsto no princípio de finalidade, os dados devem ser tratados para determinados propósitos, os quais devem ser informados ao titular dos dados previamente, de modo claro e sem que seja possível a utilização para demais fins. O princípio da adequação prevê que os dados devem ser usados de acordo com a finalidade reportada ao titular dos dados. O tratamento deve ser limitado ao mínimo necessário para a realização do objetivo cujo foi informado, como apontado pelo princípio da Necessidade (BRASIL, 2018).

O princípio do livre acesso, dispõe quanto a garantia dos titulares a consulta de maneira facilitada e gratuita sobre o modelo e o tempo de tratamento, de forma integral de seus dados. Dessa forma, os dados deverão ser entregues a seu proprietário em sua totalidade. O princípio de qualidade dos dados refere-se quanto a garantia da exatidão, clareza, relevância e atualização dos dados. Os dados colhidos, assim como os transformados por manipulação, devem ser entregues ao titular. O princípio da transparência aborda a prestação de informações claras e acessíveis pelos titulares. O proprietário, deverá ser capaz de solicitar seus dados, de alterá-los ou de solicitar sua exclusão (BRASIL, 2018).

O princípio da segurança dispõe sobre a adoção de medidas técnicas e administrativas, aptas a proteger os dados de acessos não autorizados. O art. 46, parágrafos 1º e 2º estipulam que, a Autoridade Nacional de Dados poderá dispor sobre os padrões técnicos mínimos aceitáveis, assim como sobre a responsabilidade pela adoção das medidas de proteção (BRASIL, 2018).

A GDPR introduz também o conceito de Privacy for Design criado pela Dra. Ann Cavoukian (CAVOUKIAN, 2009), que passa a ser obrigatório em processos de coleta de dados, armazenamento, transformação, circulação e uso de dados. Ressaltando que a lei é dirigida não só ao campo técnico, mas se estende ao administrativo. Desta forma, pessoas e processos também serão responsáveis pelos dados e se processamento (EUROPA, 2018).

O princípio de prevenção impõe a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Observando que não bastará mais agir de modo reativo. Se uma prevenção não for adequadamente implementada, os pressupostos jurídicos para uma ação de responsabilidade civil estarão postos: houve negligência, ou seja, descumprimento do dever geral de diligência a que todos estão subordinados (BRASIL, 2018).

O princípio de não discriminação discorre sobre a impossibilidade de tratamento de dados para fins discriminatórios. Utilizar dados para fins que geram discriminação são proibidos. A discriminação poderá ser direta ou indireta. Direta, quando a aplicação do processamento e seus resultados geraram um efeito negativo injustificável para alguém. Indireta, quando disposição, critério ou prática, aparentemente neutra, que coloque pessoas em condições de desvantagem, comparativamente a outras pessoas (BRASIL, 2018).

Por fim, o princípio de responsabilização e prestação de contas, objetiva-se na criação de Controladores de Dados, Operadores de dados e Encarregado de dados (BRASIL, 2018). Esses serão os responsáveis diretos pela empresa estar em conformidade com a nova lei. Os requisitos e impactos serão apresentados pela Autoridade Nacional de Proteção de Dados.

3.2 **AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS**

O objetivo principal da nova lei trata de garantir a segurança de dados pessoais. A lei nº13/853 altera a lei nº13/709 (LGPD) e cria a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) (BRASIL, 2019). Esse novo órgão será voltado para a proteção de dados pessoais e controle da LGPD. Ou seja, ele terá de supervisionar as instituições públicas e privadas verificando se essas obedecem às novas regras impostas pela lei. Além disso, deve zelar pela proteção dos dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (BRASIL, 2019).

A ANPD também é responsável por divulgar de forma educacional as políticas públicas de proteção de dados e suas respectivas medidas de segurança, realiza a elaboração de pesquisas e estudos sobre práticas nacionais e internacionais de proteção de dados e privacidade, análise de casos e reclamações de titular dos dados contra o controlador, cooperação com autoridades de outros países, gerenciamento da publicidade das operações de tratamento de dados, implementação de mecanismos para registros de reclamações e comunicação às autoridades sobre infrações penais. O art. 55, da LGPD fala sobre a composição do órgão ANPD que será constituída por um Conselho Diretor (órgão máximo) composto por cinco membros indicados pelo Presidente da república e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (que terá 23 representantes, titulares e suplentes, de órgãos públicos e da sociedade civil), Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e unidades administrativas para a aplicação da lei (BRASIL, 2019).

4 OS DESAFIOS AO DIREITO FUNDAMENTAL À PRIVACIDADE EM DECORRÊNCIA DOS DADOS PESSOAIS INSERIDOS NA INTERNET

O rápido desenvolvimento das tecnologias, a expansão das redes de comunicação globais e grandes mídias, corroboram para a construção de uma sociedade informacional. A amplitude dos canais de informação e comunicação pela Internet, fazem com que muitos setores se estruturam e conduzam os indivíduos a divulgarem ou compartilharem seus dados pessoais na rede, de forma direta ou captados por empresas que se utilizam desses dados para fins legítimos ou não, que Castro (CASTRO, 2005), afirma ser este cenário uma ameaça à privacidade.

Do mesmo modo que o compartilhamento dos dados facilita o uso das novas tecnologias propiciando vantagens como a maciça circulação de produtos e serviços, diminuição dos riscos e custos da atividade econômica e agilização da concessão de crédito. Essas potencialidades também apresentam riscos, com apropriação indébita de dados e/ou tratamentos que fujam do escopo acordado com o titular dos dados pessoais, refutando desta forma o ideário de privacidade.

Observa-se que as redes sociais e a Internet como um todo, têm forte poder sobre os usuários que as utilizam sem segurança e acabam colocando a sua vida privada em risco, causando muitas vezes, danos e consequências irreparáveis e inestimáveis. Não há, uma fórmula pronta

com exatidão a ser utilizada quando se tratar de privacidade seja em âmbito digital físico, ou seja, a privacidade não possui um conceito terminológico uniforme em todos os contextos, sendo complexo escapar da análise dos elementos de cada caso, para formar uma conclusão a respeito do tema e sua aplicação.

É importante destacar que no Brasil, até o ano de 2014, não havia norma específica que garantisse a privacidade das informações dos usuários que navegam no mundo virtual. Dessa forma, nos conflitos que envolvessem a violação da privacidade dos dados dos usuários na internet, aplicava-se por analogia o inciso X, do art. 5º da Constituição Federal de 1988, por não existir uma lei específica que pudesse solucionar os conflitos existentes que ocorrem através do ambiente virtual.

Diante disso, com a aprovação do Congresso Nacional, no dia 25 de março de 2014, a Lei n. 12.965/2014, conhecida popularmente como o Marco Civil da Internet, com a finalidade de regulamentar o uso da Internet no Brasil, para preencher o vazio legislativo que existia no ordenamento jurídico Brasileira sobre o assunto. O Marco Civil traz como pedra fundamental o princípio da privacidade (BRASIL, 2014).

Posteriormente foi sancionada a Lei Geral de Proteção de Dados Pessoais, para suprir as lacunas existentes nas legislações anteriores. Inspirada no GDPR, a LGPD trouxe a definição de duas figuras distintas, de agentes de dados: o controlador e o operador. No entanto, chegamos ao entendimento que é um árduo trabalho a criação de legislações que acompanhem a constante evolução da internet, atendendo aos pedidos e demandas que surgem, devido a características de instantaneidade deste novo modelo.

4.1 **DIREITO A PRIVACIDADE NA ERA DIGITAL**

A consolidação do direito à privacidade como direito fundamental, ao longo do tempo, as informações pessoais passaram a se tornar fonte de vantagens para quem as detém, sejam tais vantagens pessoais ou econômicas. O armazenamento e uso adequado dessas informações conferem maior poder de uns sobre os outros (COSTA; GOMES,2017, p. 220).

Esse é o contexto da sociedade da informação, na qual a tecnologia é considerada indispensável em todos os ramos sociais, inclusive para o desenvolvimento da própria informação e construção do conhecimento pelos indivíduos, tendo como base ideal os valores de liberdade e

comunicação. Forma-se uma nova estrutura social, de uma sociedade em rede. Observamos que o crescimento do fluxo de informações aumentou o dinamismo da sociedade e, rapidamente, a captação de informações, dados pessoais, tornou-se estratégia interessante para os entes privados com o objetivo de conhecer de forma aprofundada seus indivíduos e consumidores ou trabalhadores, respectivamente.

O interesse das corporações em adquirir informações está diretamente relacionado ao princípio da eficiência e do controle social, utilizando-se de pesquisas e censos para obtenção de maior conhecimento sobre a população e consequente aumento de seu poder de controle sobre os indivíduos. Já a importância da coleta de dados para os entes privados se evidencia a partir do desenvolvimento de tecnologias que diminuem o custo da coleta e tratamento de dados, transformando tais informações em utilidade para as empresas das mais diversas áreas de atuação, em especial às com fins comerciais e, na atualidade, com importante enfoque nas relações de trabalho (DONEDA, 2006, p. 8).

Em âmbito internacional, a Declaração Universal dos Direitos do Homem de 1948 –DUDH (UNIC, 2009) em seu artigo assegura o direito de todos terem sua vida privada resguardada sem interferências ou ataques de terceiros. O Pacto Internacional dos Direitos Civis e Políticos – PIDCP, ratificado pelo Brasil mediante Decreto 592 de 06 de julho de 1992, em seu artigo 172, garante o direito à privacidade. Em âmbito nacional, o direito à privacidade é espécie do gênero dos direitos da personalidade, regulados pelo Código Civil Brasileiro – CCB, precisamente em seu artigo 213 que trata da vida privada, e resguardados pela Constituição da República Federativa do Brasil de 1988 em seu artigo 5°, inciso X4 , que garante o direito à vida privada como direito fundamental.

O atual cenário do desenvolvimento tecnológico facilitou o acesso às informações pessoais, inclusive a dados sensíveis, tanto pelo poder público quanto por entes privados, justificando a necessidade do desenvolvimento de novas formas de proteção das informações privada. No Brasil, essa necessidade veio a ser suprida pela promulgação da Lei Geral de Proteção de Dados Pessoais, lei n° 13.709, em 14 de agosto de 2018. A lei entrará em vigor em 16 de agosto de 2020. Todavia, é importante que desde já a doutrina analise e reflita acerca de suas repercussões nos diferentes campos do direito. A LGPD, ao regulamentar a proteção de dados pessoais, garante o exercício dos direitos da personalidade, estabelecendo limites ao direito de acesso às

informações de terceiros e à utilização de tais dados com intenções discriminatórias, ilícitas ou ilegais.

4.2 **ABORDAGEM COMPARATIVA ENTRE O QUADRO REGULATÓRIO BRASILEIRO E EUROPEU**

A comparação entre a GDPR e a LGPD é uma questão de grande valor prático. Vale destacar que a GDPR pode se aplicar às empresas brasileiras, tendo em vista que seu escopo territorial abrange dados coletados de pessoais naturais que se encontram na União Europeia. O consentimento é uma base legal que se encontra em ambas as normativas. Sobre esse ponto, as normas apresentam algumas semelhanças, tais como: o consentimento por escrito deverá constar em cláusula separada das demais; a prova do consentimento é um ônus do controlador/responsável, entre outras. Uma importante diferença entre as normas é que a GDPR não caracteriza como livre o consentimento quando este se mostra como um requisito para a prestação de um serviço, enquanto a LGPD apenas destaca que o titular dos dados pessoais deve ser informado quando o tratamento de dados é condição para obtenção de um produto ou serviço.

O sistema protetivo da GDPR funda-se, de um lado, na principiologia típica da seara da proteção de dados, frisando a promoção das garantias e prerrogativas individuais implicadas na matéria, e, de outro, em determinações específicas, concretas, regras que visam à cobertura das situações fáticas já verificadas, aptas a manter-se a par do desenvolvimento tecnológico. Sendo a maior referência na matéria de proteção de dados, contando com um sistema legal e institucional avançado, cujo desenvolvimento se processou através de décadas. O direito ao esquecimento passa a ser previsto legalmente, no qual o titular pode solicitar o apagamento de seus dados numa gama de situações (PEDRO CAVALCANTE, 2018).

A LGPD pode ser vista como uma diretiva geral para a proteção de dados no Brasil. Isso significa que a nova lei busca não substituir as que existem atualmente, mas estabelecer regras e princípios gerais para que as mesmas possam ser cumpridas de uma maneira mais benéfica para o cidadão. Naturalmente, caso se verifiquem contradições entre essas leis e a LGPD, as regras clássicas para decisão entre contradições jurídicas deverão ser aplicadas (RENATO MONTEIRO, MARIA GOMES, ADRIANE NOVAES, GABRIELA MORIBE, DENNYS CAMARA, PAMELA GHERINI, 2019).

Diante de tudo isso, é possível afirmar que a LGPD, assim como a GDPR, terá um impacto na sociedade como um todo como poucas leis antes tiveram, devido a sua natureza horizontal e transversal. Importante sempre lembrar que ao mesmo tempo que a lei visa garantir ao titular, uma proteção maior no uso de seus dados pessoais, ela visa, também, fomentar o desenvolvimento econômico, tecnológica e a inovação. Tais prismas devem orientar a interpretação de lei por completo. Somente desta forma a vontade do legislador, e da sociedade, serão alcançadas. A tabela 1 (ZYGON DIGITAL, 2019) indica de forma mais prática a visualização das principais diferenças entre a GDPR e a LGPD.

Tabela 1

GDPR		LGPD
Multa de até 20 milhões de euros ou 4% sobre a receita anual global da empresa, o que for maior.	Penalizações	Mais amenas, de advertências a 2% do faturamento total da empresa.
É necessário ter um representante estabelecido em um dos Estados-membros	Representantes	Não existe nenhuma obrigatoriedade em relação ao local de estabelecimento.
São aceitas autorizações de menores com no mínimo 16 anos.	Dados de Menores de Idade	Dados de menores de 18 anos precisam de autorização do responsável para serem usados.
Obrigatório	Políticas Internas de Proteção de Dados	Opcional
Deverá ser realizado quando o tratamento dos dados oferecer risco elevado à privacidade dos mesmos. O GDPR detalha as informações que devem constar no documento.	Relatório de Impacto	Não há nenhuma especificação sobre a necessidade de um relatório do tipo.
Necessidade de um contrato que comprove o vínculo entre as duas partes.	Relação Controlador – Operador	Não é necessária a formalização do vínculo.
Regulamento específico para os dados tratados com esta finalidade	Marketing Direito	Não possui uma previsão específica nas normas.

Fonte: ZYGON DIGITAL, 2019

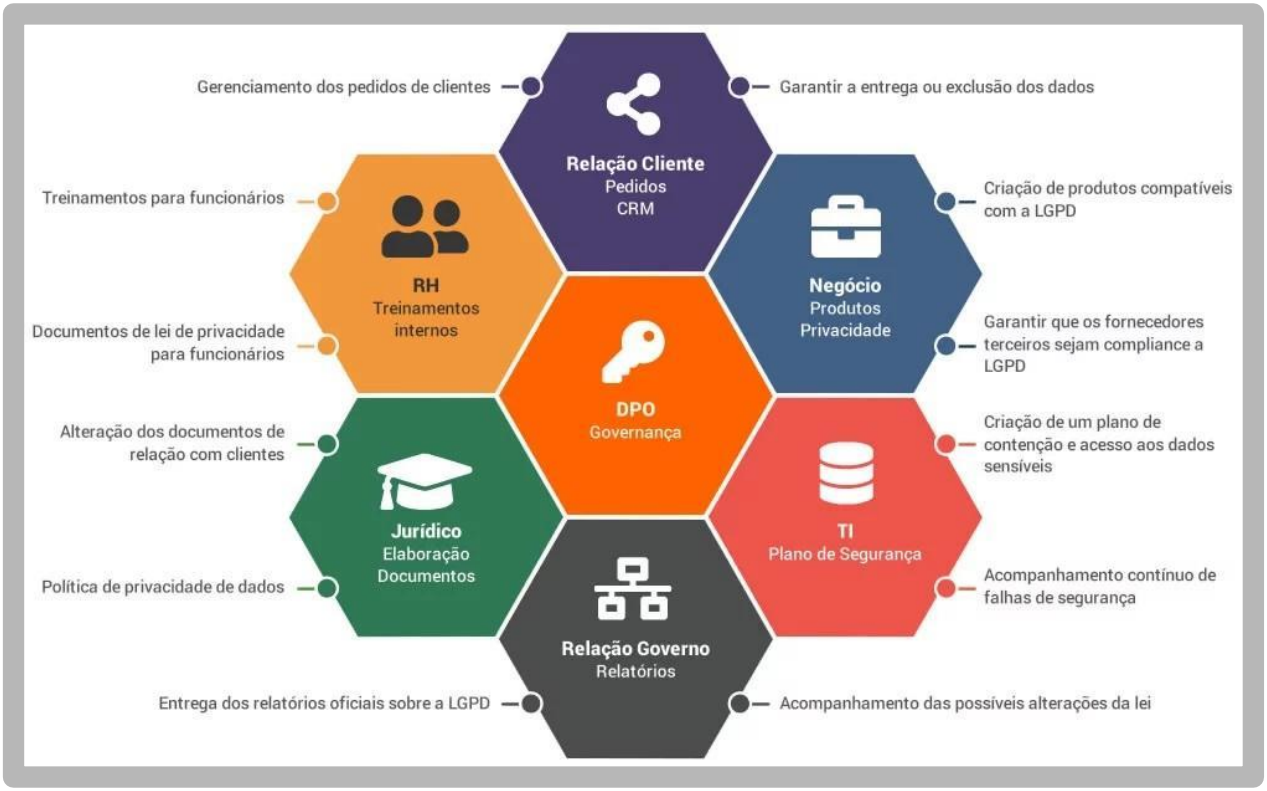
4.3 **OS IMPACTOS DA LGPD NAS EMPRESAS**

A LGPD traz diversas mudanças para o uso de dados no setor público e privado, com o objetivo de trazer uma maior segurança aos dados dos titulares. Agora as empresas poderão coletar apenas dados pessoais e identificáveis como nome, idade, endereço, e-mail, telefone, entre outros com a autorização clara do titular dessas informações. O uso desses dados também

deverá atender a vontade do titular. Logo se eles quiserem excluir, cancelar, ou alterar suas informações na base, devem ter livre acesso. As empresas são as principais responsáveis por proteger essa base de dados com medidas de segurança eficazes contra possíveis acessos indevidos aos dados. Em caso de comprometimento das informações, as punições irão variar de acordo com cada infração.

> No Art. 52º a lei prevê sanções administrativas aplicáveis pela autoridade nacional podendo ser desde uma advertência com prazo estipulado para adoção de medidas corretivas, multa de até 2% do lucro do faturamento do último exercício limitada a R$ 50.000.000,00, multa diária observado o limite total anteriormente citado, divulgação pública da infração após a devida apuração e comprovação do incidente, bloqueio dos dados pessoais referentes a infração até sua regularização e eliminação dos dados pessoais referentes a infração (BRASIL, 2018).

Figura 1



Fonte: MANDIC, 2019

Para ilustrar o impacto da LGPD em cada setor das empresas que tratam dados pessoais (veja Figura 1) (MANDIC, 2019). Nela podemos observar o impacto na relação com o cliente, negócio, tecnologia da informação, relação com o governo, jurídico e recursos humanos. Cada setor com suas especificidades. Para ajudar as empresas nessa adaptação, o encarregado (DPO

na GDPR) criado pela LGPD em seu art. 41, será responsável por ajudar na adaptação de cada setor das empresas. Também deverá atender as tarefas que a LGPD determina as quais são "aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências", "receber comunicações da autoridade nacional e adotar providências", "orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais" e "executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares" (BRASIL, 2018).

4.4 **ADAPTAÇÃO AO NOVO QUADRO REGULATÓRIO BRASILEIRO**

As empresas terão um tempo para se adaptar à nova legislação brasileira. Segundo o art. 65, da LGPD o período para adaptação é de 24 meses, iniciados a partir da data de sua publicação em agosto de 2018, ou seja, todas as empresas que tratam dados dos titulares precisam estar de acordo com a regulamentação até agosto de 2020. (BRASIL, 2018, Art. 65) Alguns pontos podem ser levados em consideração para proteção do ambiente que receberá os dados dos titulares o que torna necessário a mudança de alguns processos internos das empresas como:

1. Revisão e melhoramento de processos externos e internos de dados como gestão de dados, mecanismos de controle e auditoria, atualização de ferramentas de segurança;
2. Revisão de documentos que envolvem normas, políticas, contratos que englobam fornecedores e demais parceiros de negócio;
3. Promover uma verdadeira mudança cultural com o envolvimento de toda a empresa em treinamentos periódicos bem como a conscientização de fornecedores, parceiros e clientes.

E todo esse processo pode começar através de um diagnóstico realizado por atores internos e/ou externos. Um jurídico especializado na lei que constatará todo o processo de dados na empresa e, baseado na LGPD, avaliará possíveis riscos e inconformidades. Uma empresa de tecnologia especializada que avaliará todo o tratamento de dados pessoais de sua empresa elencando pontos de como são coletados, armazenados e compartilhados com um entendimento profundo de todo o fluxo de informação dentro e fora da empresa.

Com essa análise tecnológica e jurídica é possível compreender os pontos frágeis que a empresa tem em relação ao tratamento de dados dos titulares e como ela pode se adequar à lei criando um plano de trabalho e recomendações envolvendo ferramentas, processos, sistemas e pessoas. Após isso é preciso monitorar através do sistema, processos e treinamento de pessoas se todo o trabalho feito está sendo corretamente implementado e utilizado no dia-a-dia da empresa.

4.5 **BENEFÍCIOS DA LGPD PARA AS EMPRESAS**

A LGPD não trará apenas novos custos e prazos apertados de adaptação às novas regras além de muitas mudanças difíceis de serem implementadas. É possível abstrair pontos positivos dessa nova legislação, já que elas podem trazer benefícios para as empresas. A Reamp cita alguns desses benefícios, como por exemplo: (EQUIPE REAMP, 2018)

A LGPD reúne todas as regras relacionadas à privacidade no Brasil. Sua criação é importante para manter o mercado brasileiro no mesmo patamar que outros mercados do mundo. O mundo como um todo tende a criar leis de proteção de dados pessoais, e com isso tornou-se importante que o Brasil se adaptasse, atribuindo maior segurança jurídica (EQUIPE REAMP, 2018).

A transparência entre empresa e cliente será maior visto porque a empresa terá a necessidade de explicar melhor por quais motivos as informações dos usuários serão utilizadas gerando uma maior confiabilidade aos seus consumidores. Além disso, uma das principais razões para a criação da lei foi permitir que os usuários passassem mais tempo nos sites que desejam, sem ficarem sobrecarregados com anúncios não solicitados. Portanto, é provável que os clientes aceitem a participação de organizações e empresas de seu interesse e que não sejam invasivas na hora da abordagem. A tendência é que os usuários mantenham seus dados apenas em empresas as quais ele confia tornando-se um cliente leal a marca (EQUIPE REAMP, 2018).

As organizações vivem uma batalha sem fim pela segurança de suas redes, servidores e infraestrutura e isto têm sido uma fonte primária de proteção cibernética junto com outras alterações de políticas e segurança. Na UE a aprovação do GDPR alterou diretamente os padrões de privacidade e segurança dos dados e, ao mesmo tempo, incentivou indiretamente as organizações a desenvolverem e aprimorarem suas medidas de segurança cibernética, limitando riscos de qualquer possível violação de dados. A GDPR obriga as empresas a identificarem sua estratégia de segurança adotando medidas administrativas e técnicas adequadas para proteger os dados pessoais dos cidadãos. Por isso, essas atividades ajudarão a organização a entender melhor o que está acontecendo em sua rede, aprimorando a segurança cibernética (EQUIPE REAMP, 2018).

A LGPD também traz o benefício da melhora no gerenciamento de dados, visto que a partir de agora é necessário que cada empresa saiba exatamente quais informações possui sobre cada usuário. Por isso, uma auditoria de dados minimizando informações coletadas e mantidas

desnecessariamente e organizar melhor os dados armazenados refinando os processos de gerenciamento de dados (EQUIPE REAMP, 2018).

Com a revisão de todo o banco de dados das empresas, informações irrelevantes que atrapalham o marketing da empresa serão eliminadas como, por exemplo, endereços que não existem mais, telefones não mais utilizados, tornará o banco de dados mais organizado com os clientes mais importantes. Com informações mais fidedignas o marketing consegue adaptar mais facilmente suas mensagens levando em conta a necessidade e hábitos específicos do seu público que será melhor definido. Isso levará um aumento do seu retorno sobre o investimento (ROI), porque o orçamento do marketing será gasto de maneira mais inteligente trazendo um maior retorno as empresas (EQUIPE REAMP, 2018).

A empresa poderá se tornar uma apoiadora da privacidade dos seus clientes melhorando sua imagem perante seus clientes. As organizações devem pensar que sua marca como uma empresa que pode contribuir para a comunidade, e não apenas consome para se sustentar e crescer. Tudo isso valorizará o marketing da empresa demonstrando ao cliente sua importância. Com informações mais fidedignas o marketing consegue adaptar mais facilmente suas mensagens levando em conta a necessidade e hábitos específicos do seu público que será melhor definido (EQUIPE REAMP, 2018).

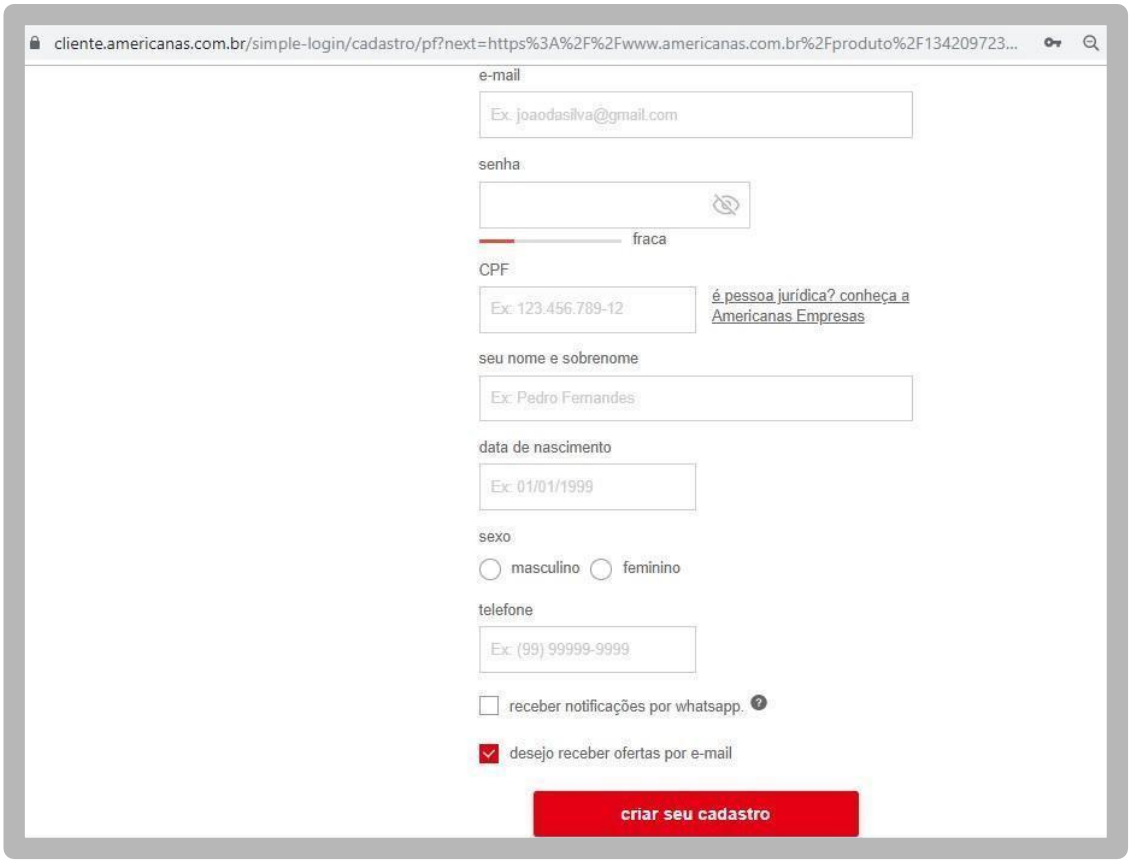
Cada cliente terá de optar objetivamente por receber campanhas da área de marketing da empresa, logo somente mais envolvidos provavelmente permanecerão no banco de dados da empresa. A empresa contatará somente os clientes mais valiosos que realmente querem ouvir e comprar com ela. As empresas que souberem se adaptar de forma mais rápida controlando seus custos e renovando seus processos podem acabar se beneficiando da LGPD e conseguindo uma boa vantagem competitiva em relação aos concorrentes (EQUIPE REAMP, 2018).

5 CENÁRIO DA APLICAÇÃO DO ESTUDO

A fim de tornarmos este estudo tangível, buscamos analisar o papel de cada ator de um processo de compras online, observamos o comportamento de um site de compras, onde um cliente deseja comprar uma impressora para sua casa. Pesquisando o produto desejado na internet ele optou em comprar no site da americanas.com.br. Para isso o cliente precisa realizar

um cadastro com suas informações pessoais, exigidas pelo site (veja Figura 2). Essas informações são: e-mail, cpf, nome, sobrenome, data de nascimento, sexo e telefone.

Figura 2



Fonte: B2W - Companhia Digital

O indivíduo observado verifica que a americanas.com.br oferece um serviço de marketplace, modelo no qual diversas outras empresas anunciam seus produtos, fornecendo aos clientes um leque de opções e variedade na oferta de preços. Os nomes de algumas das empresas que vendem a impressora são listados na página da busca realizada por produto, assim como os valores do item e do frete (veja Figura 3). No entanto caso ele deseje ver os nomes de todas as empresas com suas especificidades, a página oferece o recurso de redirecionamento que lista todas as empresas e seus respectivos valores ofertados pelo produto.

Figura 3

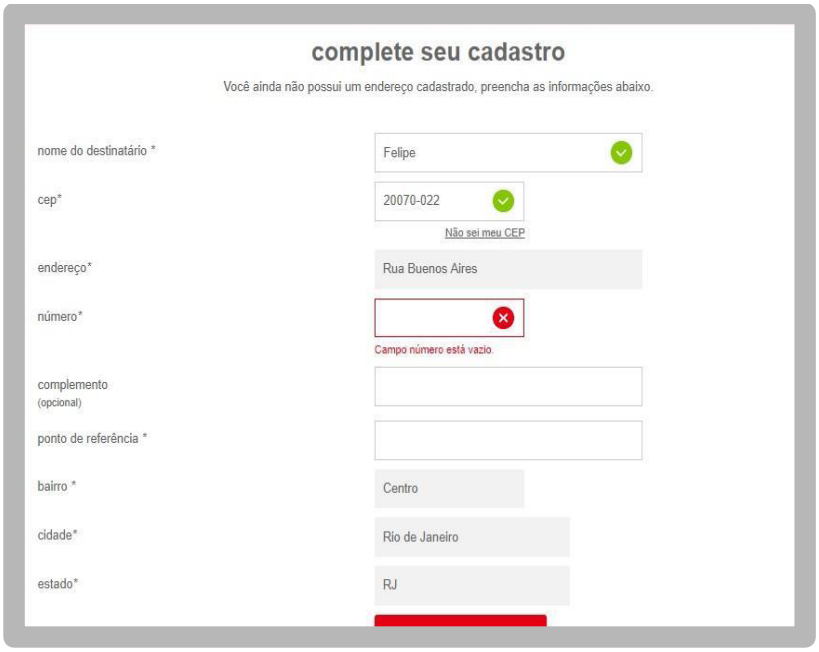
Fonte: B2W - Companhia Digital

O titular dos dados, preocupado com o possível compartilhamento de seus dados, realiza a leitura de política de privacidade do site da americanas.com.br. Nela é possível ler o seguinte texto:

> A americanas.com.br tem o compromisso com a privacidade e à segurança de seus clientes durante todo o processo de navegação e compra pelo site. Os dados cadastrais dos clientes não são vendidos, trocados ou divulgados para terceiros, exceto quando essas informações são necessárias para o processo de entrega, para cobrança, ou para participação em promoções solicitadas pelos clientes. Seus dados pessoais são peça fundamental para que seu pedido chegue em segurança, na sua casa, de acordo com nosso prazo de entrega. A americanas.com.br utiliza cookies e informações de sua navegação (sessão do browser) com o objetivo de traçar um perfil do público que visita o site e aperfeiçoar sempre nossos serviços, produtos, conteúdos e garantir as melhores ofertas e promoções para o usuário. Durante todo este processo a empresa mantém suas informações em sigilo absoluto. Vale lembrar que os dados são registrados pela americanas.com.br de forma automatizada, dispensando manipulação humana (B2W - COMPANHIA DIGITAL, 2019).

Como é possível notar, o site informa que caso o cliente observado deseje efetuar a compra da impressora, a americanas.com.br terá de compartilhar com a outra empresa de marketplace, a qual vende o produto desejado, alguns ou todos os dados pessoais do titular. O indivíduo do estudo precisa da impressora o mais breve possível e por isso ele decide escolher no site da americanas.com.br uma empresa que melhor lhe convém para compra. Após a escolha ele é redirecionado para uma página onde tem de informar outros dados, estes relativos ao seu endereço, como: cep, nome da rua, número da residência, complemento, ponto de referência, bairro, cidade e estado (veja Figura 4).

Figura 4



Fonte: B2W - Companhia Digital

Após informar seus dados, o usuário é redirecionado para uma página de pagamento na qual escolhe o modo de pagamento preferido e finaliza a compra. A LGPD em seu art. 5, criam as figuras do titular, controlador e do operador respectivamente definindo o titular como "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento", controlador como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" e o operador como "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"(BRASIL, 2018).

Retornando ao cenário acima citado podemos concluir que o titular é o cliente, o controlador é a americanas.com.br onde o cliente cadastra seus dados e o operador é o fornecedor do produto comprado. A LGPD estabelece nesse caso, que tanto a americanas.com.br quanto o fornecedor devem manter registro dessa operação de tratamento de dados pessoais do titular que realizarem, especialmente quando baseado no legítimo interesse que é o caso desse cenário apresentado.

Também é dispensado nesse caso o consentimento do titular para compartilhamento de dados entre a americanas.com.br e o fornecedor, pois se trata de um cumprimento de obrigação legal ou regulatória pelo controlador. O titular nesse caso tem direito a ter a confirmação da existência do tratamento dos seus dados pelo operador e pelo controlador bem como obter informações

das entidades privadas com as quais o controlador realizou o uso compartilhado de dados. O titular também poderá exigir a alteração ou eliminação de seus dados do banco de dados do controlador e/ou do operador.

A GDPR traz em seu artigo 4:

> Art. 4º. 11) Consentimento do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento (GDPR, 2018).

Os art. 18 e 19 da LGPD prevê que o titular dos dados pessoais possa obter do controlador, a qualquer momento, a portabilidade dos seus dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador. Estes artigos estabelecem a necessidade do consentimento ser livre, específico, informado e inequívoco. A inatividade do titular dos dados, não devem constituir consentimento para que os dados sejam tratados.

Nesse sentido, a empresa optando pelo tratamento de dados pessoais através do consentimento do titular, é recomendável o uso de pedido de consentimento destacado. No art. 16 da LGPD diz que caso o controlador tenha que realizar o cumprimento de obrigações regulatórias os dados podem não ser eliminados mesmo diante vontade expressa do titular (BRASIL, 2018). Em regra, o interesse da empresa não pode conflitar com as expectativas do titular, devendo ser adotadas medidas de controle e transparência do processo, facultando ao usuário de sistema se opor ao tratamento quando julgar propício.

6 CONCLUSÃO

O presente trabalho objetivou-se na análise das legislações aplicáveis para o tratamento de dados pessoais, bem como as precauções a serem adotadas para a sua coleta e tratamento em Big Data, explicitando com modelos de serviços de vendas distribuídos. Foram abordadas aplicações da Lei Geral de Proteção de Dados (LGPD), que entrará em vigor no ano de 2020, a qual foi estruturada com base na General Protection Regulation (regulamentação Europeia). Nesta nova legislação brasileira, são elencadas possibilidades diversas para tratamento de dados pessoais e traz inúmeras inovações sobre a questão.

Exploramos os desafios no campo do Direito, em acompanhar o ritmo da disrupção causada pelo fenômeno tecnológico. As abordagens legais que pretendem regular as situações geradas pelas inovações tecnológicas correm o risco de tornarem-se obsoletas, visto que o ritmo da disrupção é incessante. Tendo-se em conta que os dados pessoais passaram a constituir um commodity de alto valor para a era digital, a proteção destes dados surge como grande desafio frente a situações inéditas.

A análise da Lei Geral de Proteção de Dados Pessoais, sancionada recentemente, revela um quadro regulatório bem-elaborado, sintonizado com as discussões mais atuais sobre a matéria de forma ampla, isto é, cobrindo o estado tecnológico de maneira genérica. Reúnem-se, assim, as condições favoráveis ao desenvolvimento gradativo de um modelo bem-sucedido de proteção de dados pessoais. Ressaltando a importância de entidades regulatórias de proteção de dados pessoais. Esperamos que a revisão apresentada neste artigo possa oferecer aos pesquisadores, diferentes ideias sobre a questão da mineração de dados que preservam a privacidade e promova a exploração de novas soluções para a segurança de informações confidenciais.

Em trabalhos futuros, sugere-se a análise prática com estudo de campo de cunho qualitativo, da adequação de empresas à Lei Geral de Proteção de Dados a partir de sua vigência em agosto de 2020, observando as estratégias adotadas pelos mais diversos setores.

REFERÊNCIAS

B2W - COMPANHIA DIGITAL. **Política de Privacidade**. americanas.com.br. Rio de Janeiro. Disponível em: https://www.americanas.com.br/hotsite/politica-de-privacidade. Acesso em: 7 Set. 2019.

BARROSO, Luis; BARCELLOS, Ana Paula. **O começo da história. A nova interpretação constitucional e o papel dos princípios no direito brasileiro**. Revista de Direito Administrativo, Rio de Janeiro, p. 141-176, Junho 2003.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. **Lei n. 12.965, de 23 de abril de 2014**. Diário Oficial da União. Brasília, 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 7 Abr. 2019.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. **Lei n. 13.709, de 14 de agosto de 2018**. Diário Oficial da União. Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 21 Abr. 2019.

BRASIL. Presidência da República. **Lei n. 13.853, de 08 de julho de 2019**. Diário Oficial da União. Brasília, 08 de julho de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 4 Dez. 2019.

CASTRO, Catarina Sarmento e. **Direito da Informática, Privacidade e Dados Pessoais**. Coimbra: Almedina, 2005.

CAVALCANTE, Pedro Peres. **Privacidade e proteção de dados pessoais: Uma análise comparativa dos quadros regulatórios brasileiro e europeu**. Recife, 2018. Monografia (Direito) - UNIVERSIDADE FEDERAL DE PERNAMBUCO, Recife, 2018. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/34357/5/Monografia_PRIVACIDADE%20E%20PROTE%C3%87%C3%83O%20DE%20DADOS%20PESSOAIS%20-%20Uma%20an%C3%A1lise%20comparativa%20dos%20quadros%20regulat%c3%b3rios%20brasileiro%20e%20europeu%20final.pdf. Acesso em: 29 Set. 2019.

CAVOUKIAN, Ann. **Privacy by Design: The 7 Foundational Principles**. ipc.on. Ontario, Canada, 2009. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 29 Set. 2019.

COMISSÃO EUROPEIA. **Acordo sobre reforma da proteção de dados na UE proposta pela Comissão estimula mercado único digital**. ec.europa. Bruxelas, 2015. Disponível em: https://ec.europa.eu/commission/presscorner/detail/pt/IP_15_6321. Acesso em: 30 Set. 2019.

COMISSÃO EUROPEIA. **Diretiva do parlamento europeu e do conselho: relativa à acessibilidade dos sítios Web dos organismos do setor público**. Bruxelas, 2012. Disponível em: https://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0721/COM_COM(2012)0721_PT.pdf. Acesso em: 21 Set. 2019.

COSTA, Andréa Dourado; GOMES, Ana Virginia Moreira. **Discriminação nas relações de trabalho em virtude da coleta de dados sensíveis**. Londrina, 2017. Disponível em: . Acesso em: 30 Out. 2019.

ROLIM, Luciano. **Curso de Direito Administrativo**, 12ª edição, Malheiros, 2000, p. 748.

CYBERWAR: **The threat from the internet. Economist**, 3 Jul 2010. Disponível em: https://www.economist.com/leaders/2010/07/01/cyberwar

DAHN, Shannon. **Fair Information Practice Principles (FIPPS): Privacy Lead, Transformation Office of Privacy**. dhs.gov. 2008. Disponível em: https://www.dhs.gov/sites/default/files/publications/consolidated-powerpoint-final.pdf. Acesso em: 29 Set. 2019.

DOMO. **Data Never Sleeps**. 2018. Disponível em: https://www.domo.com/solution/data-never-sleeps-6. Acesso em: 22 Set. 2019.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico, Joaçaba, p. 91-108, Dez 2011.

EQUIPE REAMP. **Quais são os impactos e benefícios da LGPD para as empresas?** São Paulo, 2018. Disponível em: https://www.reamp.com.br/blog/2018/08/quais-sao-os-impactos-e-beneficios-da-lgpd-para-as-empresas/. Acesso em: 3 Ago. 2019.

EUROPA. UNIÃO EUROPEIA. **Lei n. 679, de 27 de abril de 2016.** Jornal Oficial da União Europeia, 25 de maio de 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 7 Abr. 2019.

GÜNTHER ET AL, Wendy Arianne. **Debating big data: A literature review on realizing value from big data**. sciencedirect. 2017. Disponível em: https://www.sciencedirect.com/science/article/pii/S0963868717302615. Acesso em: 9 Jun. 2019.

LANEY, Doug. **3d Data Management: Controlling data Volume, Velocity and Variety.** gartner. 2001. Disponível em: https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf. Acesso em: 8 Jun. 2019.

MANDIC. **Lei geral de proteção de dados lgpd.** 2019. Disponível em: https://www.mandic.com.br/servicos/lei-geral-de-protecao-de-dados-lgpd/. Acesso em: 29 Set. 2019.

MARTINS, Daniel. **BigData, revolução digital e o Direito.** mercurylbc. 2019. Disponível em: http://mercurylbc.com/bigdata-revolucao-digital-e-o-direito/. Acesso em: 4 Mai. 2019.

MCGRAIL, km; GUTTERIDGE, k; MEAGHER, nl. **Building on principles: the case for comprehensive, proportionate governance of data access.** Medical data privacy handbook, p. 737-64, 2015.

MERCURY LBC. **Os princípios da Lei Geral de Proteção de Dados e aplicabilidade**. mercurylbc. 2019. Disponível em: http://mercurylbc.com/os-principios-da-lei-geral-de-protecao-de-dados-e-aplicabilidade/. Acesso em: 7 Set. 2019.

MONTEIRO, Renato Leite et al. **Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos.** São Paulo, 2019. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf. Acesso em: 29 Set. 2019.

MOONEY SJ, Pejaver v. **Big data in public health: terminology, machine learning, and privacy.** Annu Rev Public Health 2018; 39:95-112.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração universal dos direitos humanos.** nacoesunidas. 2009. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 3 Ago. 2019.

ROLIM, Luciano Sampaio Gomes. **Colisão de direitos fundamentais e princípio da proporcionalidade.** Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 7, n. 56, 1 abr. 2002. Disponível em: https://jus.com.br/artigos/2855. Acesso em: 14 dez. 2019.

TECHAMERICA FOUNDATION'S. **Demystifying Big Data: A Practical Guide To Transforming The Business of Government.** bigdatawg. Washington, 2012. 10 p. Disponível em: https://bigdatawg.nist.gov/_uploadfiles/M0068_v1_3903747095.pdf. Acesso em: 9 Jun. 2019.

TEUFEL III, Hugo; OFFICER, Chief Privacy. **Privacy Policy Guidance Memorandum**. dhs.gov. 2018. Disponível em: https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-01_0.pdf. Acesso em: 29 Set. 2019.

WESTCON. **Quais os benefícios do big data analytics para os negócios?** Brasil, 2019. Disponível em: https://blogbrasil.westcon.com/quais-os-beneficios-do-big-data-analytics-para-os-negocios. Acesso em: 12 Out. 2019.

ZYGON. **gdpr x lgpd.** zygon.digital. Salvador, 2019. Disponível em: https://zygon.digital/2019/04/11/gdpr-x-lgpd/. Acesso em: 27 Out. 2019.

APÊNDICE A – Lista de ilustrações

APÊNDICE B – Lista de tabelas