

## LEI GERAL DE PROTEÇÃO DE DADOS, LEI DE ACESSO À INFORMAÇÃO E A IMPROBIDADE ADMINISTRATIVA: UM NOVO CENÁRIO PARA O AGENTE PÚBLICO NA SOCIEDADE DA INFORMAÇÃO

Fretz Sievers Junior

### RESUMO

O presente artigo tem como objetivo analisar a Lei de Geral de Proteção de Dados - LGPD (Lei 13.709 de 2018) que entrará em vigor, em 3 de maio de 2021, através da Medida Provisória (MP) nº 959/20, que visa resguardar os dados sensíveis das pessoas físicas e jurídicas e a Lei de Acesso à Informação Lei nº 12.527, de 18 de novembro de 2011 que já está em vigor, a qual tem como objetivo dar publicidade as informações de interesse público através da publicação de informações públicas através dos sítios eletrônicos da Administração Pública, como por exemplo a remuneração dos agentes públicos. A primeira lei visa a proteção dos dados, visando resguardar a privacidade e a segunda visa a publicidade, neste sentido o artigo visa esclarecer um conflito aparente de princípios constitucionais referentes aos dados do agente público. A lei de Improbidade Administrativa protege os bens públicos e visa punir o agente que tiver enriquecimento ilícito em seu artigo 9º, cometer danos ao erário, artigo 10º e a violação dos princípios da administração pública no artigo 11 da Lei nº 8.429, de 2 de junho de 1992. Com a evolução Sociedade da Informação, através das tecnologias da informação, o funcionário público tem um novo cenário na proteção dos dados sensíveis e caso a LGPD não seja cumprida poderá responder pelo ilícito de improbidade administrativa previsto no artigo 11. O artigo visa debater esse novo cenário para o agente público.

**Palavras chaves:** Lei Geral de Proteção de Dados. Lei de Acesso à Informação. Lei de Improbidade Administrativa. Agente Público. Direito Administrativo. Sociedade da Informação

### ABSTRACT

The purpose of this article is to analyze the General Data Protection Law - LGPD (Law 13,709 of 2018) that will come into force on May 3, 2021, through Provisional Measure (MP) No. 959/20, which aims to safeguard the sensitive data of individuals and legal entities and the Law of Access to Information Law No. 12,527, of November 18, 2011, which is already in force, which aims to publicize information of public interest through the publication of public information through public administration websites, such as the remuneration of public agents. The first law aims at data protection, aiming to protect privacy and the second aims at advertising, in this sense the article aims to clarify an apparent conflict of constitutional principles referring to public agent data. The Administrative Improbability Law protects public assets and aims to punish the agent who has illicit enrichment in Article 9, to commit damages to the treasury, Article 10 and the violation of the principles of public administration in Article 11 of Law No. 8,429, of June 2 1992. With the evolution of the Information Society, through information technologies, the civil servant has a new scenario in the protection of sensitive data and if the LGPD is not complied with, he will be able to answer for the administrative misconduct provided for in article 11. The article aims to debate this new scenario for the public agent.

**Keywords:** General Data Protection Law. Access to Information Law. Administrative Improbability Law. Public Agent. Administrative law. Information Society

### 1. Introdução

Com a evolução da Sociedade da Informação, baseado em ciência da computação, novas tecnologias vêm mudando mundo, oferecendo produtos e serviços de forma de on-line baseado em tecnologia da informação. Novos conceitos surgem no mundo moderno tais como

*bigdata*, internet das coisas, inteligência artificial, realidade aumentada etc. Essas tecnologias podem estar no setor público, através de contratos com a administração pública e no setor privado através da competitividade do mercado.

*BigData* em apertada síntese é uma grande quantidade de dados que se encontra na rede mundial de computadores, sendo que muitos dados são colhidos por diversos dispositivos eletrônicos. É baseado em volume pela sua quantidade de dados, aproximadamente exabyte (EB) que comporta  $1024^{15}$  bytes. Os dados encontram-se em uma variedade de formatos que podem estar em formato de dados não estruturados: vídeos, planilhas, textos etc., e dados estruturados que se encontram armazenados em banco de dados. Apesar da quantidade de dados, a velocidade referente ao tempo de acesso desses dados deve ser rápida e por fim outra propriedade e a veracidade, se os dados são confiáveis ou não. Um exemplo desses dados são os processos eletrônicos que se encontram nos diferentes tribunais.

A Internet das Coisas vem interligando todos os tipos de objetos eletroeletrônicos, tais como fogão, geladeira, freezer etc. Esses equipamentos podem colher diversos de informações, como por exemplo a geladeira com um software embarcado e um microcontrolador, poderá informar o tipos de produtos que uma pessoa gosta de consumir, e fazer uma lista de compras para o supermercado e encaminhar para o celular ou mesmo através de uma programação emitir uma ordem de compra para o supermercado de sua escolha e lhe informar o dia que será sua entrega. No caso da área jurídica, através da tecnologia de rádio frequência, é possível colocar uma etiqueta eletrônica de rádio frequência (RFID) para saber a localização física de um processo e sua situação sem ter a necessidade de remover o processo físico do cartório, ou mesmo o próprio processo as palavras poderão estar conectadas em uma base com ontologia que dará significado para as máquinas e ela gerar uma petição inicial referente aos fatos relatados.

A Inteligência Artificial visa colocar características humanas nos computadores. Nos documentos eletrônicos pode-se utilizar Web Semântica que visa dar significado as palavras de um texto para as máquinas, como por exemplo dar a diferença de um procedimento administrativo de um processo administrativo.

Na Administração Pública, a Lei de Acesso à Informação - LAI (Lei nº 12.527, de 18 de novembro de 2011) determina uma forma de cumprir o princípio da publicidade que se encontrado no artigo 37 da Constituição Federal, que os dados referentes a gastos públicos estejam disponíveis a qualquer pessoa sem que seja feito nenhum tipo de pedido.

Para ter acesso basta entrar no sítio da administração pública e realizar uma consulta. O portal da transparência do Governo do Estado de São Paulo<sup>1</sup>, o qual pode-se ter acesso aos gastos públicos dos agentes públicos (remuneração mensal, seus cargos e funções, diárias e passagens), despesas realizadas com a pandemia (gastos realizados ao combate do covid-19 e seus efeitos), administração pública (patrimônio, concurso público, etc).

Nesse cenário vem a pergunta: Quais são os tipos de dados sensíveis do agente público estão sendo divulgados através da rede mundial de computadores? Como esses dados estão sendo tratados e quais informações estão disponibilizadas? Até que ponto o princípio da publicidade da administração pública, em tese fere o princípio da intimidade do agente público? O agente público tem direito à privacidade referente ao cargo, emprego ou função que exerce?

A partir do dia 03 de maio de 2021, conforme a Medida Provisória nº 959/2020 que alterou a *vacatio legis* da Lei de Proteção de Dados, Lei 13.853 de 08 de julho de 2019, que visa a proteção de dados sensíveis, ou seja dado que propiciam o reconhecimento de uma pessoa, seja ela física ou jurídica.

Em um mundo totalmente dependente de tecnologia da informação onde o software está em todos os lugares, seja nos veículos automotores, *smartphones*, *smartwatches*, *smartTV*, *smartwatchs*, *etc*, que através da rede mundial de computadores, permitem saber em que local cada pessoa se encontra seja pelo GPS (*General Position System*), ativado em seu *smartphone*, ou por câmeras espalhadas pela cidade, fica a pergunta: quais os dados estão sendo capturados e para qual finalidade? Esses dados são sensíveis ou não?

E neste contexto referente ao agente público tem-se a Lei de Improbidade Administrativa, LEI Nº 8.429, DE 2 DE JUNHO DE 1992, sendo o ato improprio aquele que é desonesto e vem de encontro a proteção da Administração Pública contra o enriquecimento ilícito (art. 9º), lesão ao erário (art.10) , benefícios financeiros e tributários indevidos (10-A) e ferir os princípios da administração pública (art. 11) que estão previsto no artigo 37 da Constituição Federal.

Com a força da LAI e da LIA surgiu a fiscalização social, ou seja, qualquer cidadão poderá ter acesso aos dados da administração pública e questionar os seus feitos e também realizar denúncias a supostas irregularidades através dos sites de departamento público pelas ouvidorias, que podem ensejar a procedimentos administrativos, sindicâncias, inquéritos civis e por fim a Ação de Improbidade Administrativa que poderá penalizar o agente público casando

<sup>1</sup> Portal da Transparência, disponível em <http://www.transparencia.sp.gov.br/>

seus direitos políticos, penalidades de suspensão, perda do cargo público e não poder prestar serviço para administração pública por 5 anos.

Visando a importância do tema, o CNJ – Conselho Nacional de Justiça (GOMES,2015), realizou uma pesquisa intitulada: “Lei de Improbidade Administrativa – Obstáculos à plena efetividade do combate aos atos de improbidade”, a qual visa verificar entre outras análises, o número de ações com o tema improbidade administrativa com pedidos julgados procedentes. Isso mostra a importância do tema para o país, o qual gera prejuízos a toda população brasileira e problemas ao agente público.

Nesse novo cenário em que a sociedade vive, queremos responder a questão referente quais são as ferramentas que podem ser utilizadas para o controle social, visando a fiscalização dos gastos públicos e o que deve ser feito que o agente público não venha a cometer nenhum ato de improbidade administrativa, que gera inúmeros problemas para sua vida em particular e também para toda a população.

A seguir iremos responder com nossas pesquisas o aparente conflito entre o princípio da publicidade e da privacidade referente aos dados do agente público.

## **2. Aparência de conflitos entre os princípios da publicidade e da privacidade na Sociedade da Informação referente ao agente público.**

O direito da privacidade previsto no artigo 5º, inciso X que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurados o direito de indenização pelo dano material ou moral decorrente de sua violação”. Porém com a evolução da tecnologia, como os celulares muitos de nossos dados são coletados de forma pervasiva, ou seja, não se percebe que estamos interagindo com o ambiente, pois o gps poderá dar a nossa posição a qualquer tempo e em qualquer lugar.

Um exemplo é quando estamos conectando a uma rede sem fio, de um estabelecimento comercial que muda de antena sem a interação com o usuário. Ou quando acessamos os sites da internet para preencher um cadastro com nossos dados e não se sabe o que será feito com aqueles dados. Eles podem ser utilizados para diversos fins, como a captura de likes de uma rede social para saber as nossas preferências e oferecer produtos e serviços em momentos que estamos acessando uma rede social.

Nesse sentido visando, proteger os dados das pessoas a LGPD, protege o que chama-se de dados sensíveis referente a identificação da pessoa, tais como seus dados pessoais como o número de cadastro de pessoa física (cpf) e registro geral (rg), mas há outros dados sensíveis tais como religião, o qual a pessoa poderá sofrer algum tipo de preconceito.

O Código Civil em seu artigo 21 versa: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a essa norma”. Porém em um mundo onde os estabelecimentos comerciais possuem câmeras nas quais é possível realizar reconhecimento do local onde a pessoa esta e qual o horário que ela passou por um estabelecimento comercial.

Referente ao agente público, os seus vencimentos são publicados no portal da transparência junto com seu nome e o local em que ele trabalha. Mas esses não são dados sensíveis no qual a LGPD quer proteger?

Conforme ensinam Aras Neto (2019), Fazzio (2016) e Gasparini (2012), o princípio da publicidade visa que todos os atos do agente público sejam realizados com transparência referente a coisa pública. Nesse sentido administrar requer que todos os documentos em qualquer tempo possam ser acessados, verificados e validados por qualquer pessoa e pode ser questionado a qualquer tempo. Sendo que a publicidade torna-se possível os efeitos externos como no caso do controle social.

Nesse sentido pode-se concluir que não há privacidade quando se trata de dados da gestão pública pois os atos públicos precisam ser transparentes, neste caso o ato administrativo de um agente público deverá ser fundamentado e devidamente identificado o agente público que executa esse ato, para que qualquer pessoa possa questionar esse ato. Em caso de denúncia de um possível mal feito, haverá sempre o princípio do contraditório e da ampla defesa.

Com a evolução rede mundial de computadores surge a necessidade de regularizar a internet, sendo que Marco Civil da Internet Lei 12.965 de 2014 que visa garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria e normatiza os direitos e deveres referentes aos dados pessoais e a privacidade dos usuários, como se encontra no artigo 3º inciso II, sendo que um dos princípios e a proteção da privacidade e no inciso III a proteção dos dados pessoais. Não sendo tão precisa como a Lei Geral de Proteção de Dados.

A publicação de dados referente a qualquer pessoa natural na internet pode trazer uma certa insegurança ou desconforto e alguns dados sensíveis dos agentes públicos como seu nome e rendimentos são publicados em sítios como o site da transparência do Governo do Estado de São Paulo. Alguns agentes públicos também poderiam não gostar de ter seus rendimentos publicados na internet. Aqui apresenta-se um aparente conflito de normas constitucionais, sendo de um lado o direito à privacidade do agente público e outra o princípio da publicidade da Administração Pública em relação ao direito de informação dos cidadãos e o dever de transparência dos gastos públicos.

O Superior Tribunal Federal se pronunciou sobre a publicação do nome e da remuneração dos agentes públicos por intermédio do julgado de Repercussão Geral nº 483<sup>2</sup> assim ementado: “CONSTITUCIONAL PUBLICAÇÃO, EM SÍTIO ELETRÔNICO MANTIDO PELO MUNICÍPIO DE SÃO PAULO, DO NOME DE SEUS SERVIDORES E DO VALOR DOS CORRESPONDENTES VENCIMENTOS. LEGITIMIDADE”. Sendo que a decisão foi: “É legítima a publicação, inclusive em sítio eletrônico mantido pela Administração Pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias”. Sendo o voto do ilustre Ministro Carlos Ayres Britto o que segue:

Caso em que a situação específica dos servidores públicos é regida pela 1ª parte do inciso XXXIII do art. 5º da Constituição. Sua remuneração bruta, cargos e funções por eles titularizados, órgãos de sua formal lotação, tudo é constitutivo de informação de interesse coletivo ou geral. Expondo-se, portanto, a divulgação oficial. **Sem que a intimidade deles, vida privada e segurança pessoal e familiar se encaixem nas exceções de que trata a parte derradeira do mesmo dispositivo constitucional (inciso XXXIII do art. 5º)**, pois o fato é que não estão em jogo nem a segurança do Estado nem do conjunto da sociedade. 2. **Não cabe, no caso, falar de intimidade ou de vida privada, pois os dados objeto da divulgação em causa dizem respeito a agentes públicos enquanto agentes públicos mesmos; ou, na linguagem da própria Constituição, agentes estatais agindo “nessa qualidade”** (§ 6º do art. 37). (ARE 652777/SP,2015, p. 9, grifo nosso).

A fundamentação está embasada no princípio da publicidade sendo que o interesse público prevalece sobre o individual e essas informações interessa a todos os cidadãos. Sendo que divulgar seus rendimentos não ameaça sua vida privada e a segurança pessoal e familiar e que não se tratam de decisões previstas no dispositivo constitucional (inciso XXXIII do art 5º).

<sup>2</sup> Disponível em

[http://stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=\(652777.NUME.%20E%20ARE.SCLA.\)&base=baseAcordaos](http://stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=(652777.NUME.%20E%20ARE.SCLA.)&base=baseAcordaos), acessado em 29/04/2020



Os agentes públicos agem conforme o (§ 6º do art. 37) que estão representando o Estado na prestação de seus serviços e sendo a publicidade um dos princípios do caput do art. 37 da CF.

Os dados que se encontram no sítios públicos respeitando a Lei de Acesso a Informação, armazenam um grande volume de dados, sendo possível realizar cruzamento dos dados que se encontram em um sítio da Administração Pública com outros dados que se encontram nas redes sociais e conseguir outras informações referentes ao agente público, que muitas vezes são divulgadas por ele mesmo de sua vida privada, a qual se divulga amigos, parentes, educação, família, áreas do seu domicílio, passando uma parte de sua vida privada sendo de conhecimento público. Com a Sociedade da Informação cada um possui um conceito de privacidade, sendo que uns gostam de mostrar seu particular nas redes sociais e outros não. Com a internet a pessoa poderá tornar algo que considera privado em público, utilizando as redes sociais.

O mesmo acontece com o agente público que terá publicidade de seus dados sensíveis pelo fato do interesse público, pois ele está prestando um serviço público e que estes dados poderão ser relacionados a outros dados de suas redes sociais.

### **3. Cenário do Agente Público referente a Lei de Acesso à Informação – LAI e a Lei de Improbidade Administrativa - LIA**

A Lei de Acesso à Informação - LAI (Lei nº 12.527, de 18 de novembro de 2011) vem atender o princípio da Administração Pública que visa a transparência e a publicidade. Antes da LAI, a Administração Pública precisava ser provocada para apresentar os dados da gestão pública, mas após a LAI, basta acessar os sítios da Administração Pública para ter acesso as informações, propiciando o controle social, conforme se encontra no artigo 3º da LAI.

Dados sensíveis são os atributos relacionados a uma pessoa que trazem informações que permitem a classificação que pode gerar discriminação ou identificação. Pode-se citar como exemplo dados referentes a religião, sendo que o Brasil é um país laico, através de base de dados pode-se classificar pessoas por sua religião tanto para oferecer produtos e serviços como para atos ilícitos como preconceito. Ou sobre um determinado partido político para tentar influenciar pessoas a votar ao candidato da oposição, através de propagandas enviadas por ferramentas de comunicação (WhatsApp, Menssenger, Redes Sociais, etc).

A publicação das remunerações dos agentes públicos federais e dada pelo Decreto nº 7.724 em seu artigo 7º § 3º, inciso VI alterado em 2019 pelo Decreto 9.690 de 2019 que

determina a publicação da remuneração e subsídios recebidos por ocupantes de cargo, posto, graduação, função e emprego público

Por sua vez, o Governo do Estado de São Paulo, atendendo à Lei de Acesso à Informação, promulgou o Decreto nº 58.052/2012, aliado ao Decreto nº 61.175/2015, que em seu artigo 24 que determina que o Portal da Transparência deverá conter as entre outras informações as seguintes: relação dos agentes públicos dos órgãos e entidades da Administração Pública Direta, Indireta e Funcional, tabela de remuneração mensal dos agentes públicos dos órgãos e entidades da Administração Direta, Indireta e Fundacional, manual de navegação, glossário, perguntas frequentes, denúncias eletrônicas e “fale conosco”, por e-mail, carta e telefone.

Com os dados divulgados pelo portal da transparência, é possível que qualquer cidadão possa ter acesso aos dados e analisar situações de indícios de acúmulo de cargos ilegais ou mesmo de incompatibilidade de horários, o qual o agente público poderá responder pela tese da Improbidade Administrativa. Para isso basta formular uma denúncia de forma anônima para o órgão da Administração Pública.

A Lei de Improbidade Administrativa, (Lei nº 8.429, de 2 de junho de 1992), vem com o intuito punir os maus feitos na administração pública. Referente ao caso de acúmulo de cargos de forma ilegal está desrespeitando o artigo 37 inciso XVI que versa: “é vedada a acumulação remunerada de cargos públicos, exceto quando houver compatibilidade de horários, observando em qualquer caso o disposto no inciso XI”, o qual é permitido a acumulação legal de dois cargos de professor, de um cargo de professor com outro, técnico ou científico, de dois cargos ou empregos privativos de profissionais de saúde, com profissões regulamentadas.

A acumulação ilegal de cargos públicos fere, em tese, o princípio da legalidade, sendo um dos princípios da Administração Pública encontradas no caput do artigo 37 da CF, e que esta prevista na Lei de Improbidade Administrativa, sendo que essa também se esbarra na imprecisão que pode ser pelo fato de um erro administrativo ou mesmo uma conduta negativa, sendo que nem todo o ato ilegal tem carga negativa para uma conduta improba. Sendo que o erro administrativo não se deve ser considerado como improbidade sendo algo muito mais grave.

A lei de Improbidade Administrativa protege os princípios da administração pública em seu artigo 11, mais em específico os de honestidade, imparcialidade, legalidade as instituições conforme ensinam (ZIMMER, 2018).

Pelo fato do fácil acesso aos portais públicos a também um outro contexto tendo o agente público um desafeto que sua intenção de prejudicá-lo, poderá utilizar do meio do controle social para formular uma denúncia inverídicas, visando somente prejudicar o agente público.

Para esses casos, controle interno que muitas vezes é composta por uma unidade processante que são pessoas que vão verificar os fatos narrados na denúncia para realizar um pedido de instauração de sindicância para o levantamento de dados referente aos fatos narrados, para que se possa saber o seu ocorrido.

A próxima seção será uma análise da Lei de Proteção de Dados e a Lei de Improbidade Administrativa referente aos dados do agente público.

#### **4. Cenário referente a Lei de Geral de Proteção de Dados – LGPD e a Lei de Improbidade Administrativa**

A Lei Geral de Proteção de Dados (Lei 13.709 de 2018) em seu artigo 2º visa proteger os dados das pessoas naturais através do respeito a privacidade, autodeterminação informativa, a liberdade de expressão, de informação, de comunicação de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, dos direitos humanos, o livre desenvolvimento, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Que são os princípios de se encontra em nossa Carta Magna, que garantem a dignidade da pessoa humana e o desenvolvimento econômico e tecnológico que são necessários para o país.

A Sociedade da Informação traz um novo cenário de um mundo da era digital onde a maioria de nossas ações são documentadas pelo meio digital, seja por posições do GPS do celular onde pode informar o seu local e te oferecer produtos e serviços e como saber em que local qualquer pessoa está. Muitas de nossas interações é realizada de forma pervasiva (sem necessidade de ações). As pessoas interagem com o ambiente sem a necessidade de informar nada somente se movimentando e geram dados captados através de uma rede de sensores ou antenas sendo que as informações são passadas pelo seu dispositivo móvel. Um exemplo é a pessoa entrar em um banheiro com a luz apaga e um sensor de presença detecta sua presença sem a necessidade de pressionar nenhum botão.

Através das ferramentas de comunicação as conversas são documentas em formato texto ou digitalizadas através de gravadores de voz que se encontram nos dispositivos móveis.

Em caso da instalação de um software malicioso, elas podem ser também interceptadas utilizando software que se instalam em qualquer dispositivo através de e-mails enviados para as pessoas com softwares maliciosos com a intenção de capturar dados como senhas, arquivos, imagens, etc. Como foi os casos noticiados pela mídia referente a suposta invasão do celular do Ex Ministro da Justiça Sergio Moro<sup>3</sup>

O mundo digital trouxe muitas facilidades, mas com ele trouxe novos problemas tais como mapeamento de perfis das pessoas através de suas escolhas. Somos monitorados 24 horas seja por interação através de sítios da internet ou por redes sociais e através de softwares maliciosos. Os cliques de nossas escolhas em uma rede social informam nossas preferências e gostos por compras, filmes, humor, entre outros. Diante desse contexto a LGPD vem para prevenir que os dados coletados de forma não autorizada, sejam utilizados somente com o consentimento de seus proprietários.

Quando não são os dispositivos móveis são as câmeras que estão instaladas no comércio, ou mesmo sistemas de radares inteligentes que permitem através de reconhecimento de imagens identificar por onde um determinado veículo passou. Muito utilizado pela polícia para reconhecimento de roubos e furtos, sendo que nesse caso a informação está sendo utilizada em benefício da população referente a segurança pública.

Robôs (que podem ser hardware ou softwares) são utilizados para o atendimento de pessoas e a realização de cobranças. Ligam para as casas perguntando sobre pessoas que estão em débito, e alguns robôs têm algoritmos de reconhecimento de voz e interação e captam dados referente as respostas das pessoas. Um exemplo da utilização desses robôs e no uso do telemarketing, o qual capturam dados referente a escolhas dos produtos e serviços, sendo que esses dados são utilizados algoritmos de *datamining* (algoritmos de mineração de dados para reconhecer padrões de dados tais como padrões de compras, como por exemplo que compra carne, geralmente compra carvão para fazer churrasco em um final de semana). Com esses dados o comércio poderá oferecer produtos e serviços para os seus clientes.

Referente a mineração de dados o artigo 3º da LGPD, trata sobre esse assunto que versa sobre qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independente do meio, do país de sua sede ou de país onde esteja localizado os dados. A lei visa proteger o tratamento de dados que podem cruzar informações de diversas bases de dados, como por exemplo uma empresa que capta a localização de uma

<sup>3</sup> <https://exame.com/brasil/hacker-confessa-ter-invadido-celular-de-moro-e-centenas-de-autoridades/>, acessado em 04/07/2020



pessoa poderá relacionar essa posição sobre um mapa de uma cidade e saber suas preferências de consumo e quais produtos e serviços a loja poderá oferecer dependendo do contexto que se encontra. Talvez a proprietária dos dados não queira esse tipo de serviço, e não queira que seus dados sejam usados para esse fim, essa seria uma forma de invasão de privacidade.

A LGPD, conforme versa seu artigo 4º não é aplicada para o tratamento de dados pessoais, realizado por pessoa natural para fins exclusivamente particulares e não econômicos. Neste caso a lei permite o uso de dados para diversos fins como por exemplo fins educacionais e científicos sem fins lucrativos, o qual pede para que se atenda aos requisitos dos artigos 7º e artigo 11º da LGPD. Deve-se pedir um termo de consentimento para o titular, que nestes termos deve constar para qual o fim os dados serão utilizados e pedindo autorização de utilização desses dados para o proprietário, pode-se informar também como estes dados serão eliminados evitando que eles sejam utilizados para outros fins.

Esse termo de consentimento é muitas vezes utilizado em para trabalhos acadêmicos por estudantes em seus trabalhos de finais de curso, utilizando a coleta de dados através de formulários para que a pessoa que está sendo entrevistada possa saber para que fins está sendo utilizado seus dados.

Referente ao tratamento de dados pessoais pelo poder público, o qual se refere a LAI – Lei de Acesso a Informação, é recepcionado pelo art. 23 inciso I, pedindo que sejam fornecidas informações claras e atualizadas sobre a previsão legal em veículos de fácil acesso, preferencialmente nos sítios da internet e que seja informado quem é o encarregado e quando for realizado o tratamento de dados pessoais. Neste caso os dados fornecidos nos sítios eletrônicos terão que ter o responsável pelo tratamento dos dados dando publicidade a responsabilidade do agente público no caso da Administração Pública. A lei também cita o controlador, sendo aquele que irá cuidar dos dados dentro da empresa.

A lei pretende proteger alguns tipos de dados referentes a dignidade da pessoa humana que são considerados como dados sensíveis, como por exemplo a de origem racial ou étnica para evitar qualquer tipo de preconceito ao grupo ou uma classe específica. Como é o caso também da convicção religiosa de uma pessoa, sendo o país laico e todos tem liberdade de escolher sua religião, conforme encontra-se do art. 5 inciso VI da Constituição Federal.

Visa proteger dados referente a opinião política, para que não tenha riscos de influencia a escolha de uma pessoa para votar em um determinado candidato e nem tentar manipular sua opinião através de possíveis envios de propagandas.

Dados referentes a saúde também são protegidas por essa lei, como por exemplo o prontuário médico que traz dados sobre um paciente. São informações sigilosas armazenadas em sistemas de informação de clínicas médicas ou hospitais sejam ele público ou particular. No caso de um hospital público os agentes públicos precisam proteger esses dados, sendo permitido o acesso apenas as pessoas autorizadas.

A opção sexual de uma pessoa deve ser preservada para evitar todos os tipos de preconceito. Dados biométricos tais como impressões digitais, mão, voz, íris e outras medidas do corpo devem ser preservadas, pois esses dados são utilizados para a identificação de uma pessoa como é o caso das digitais que são utilizadas em agências bancárias em caixas eletrônicos ou mesmo em urnas eletrônicas em sistemas de votação.

Um dado anonimizado, são dados classificados como sensíveis que receberam algum tipo de tratamento, que pode ser um algoritmo de criptografia (que ira cifrar os dados permitindo a decodificação somente quem tem a chave para decifrar para saber o seu significado).

Todos os dados que a lei protege são dados que podem ser encontrados em um banco de dados, sendo um conjunto estruturado, relacionados através de campos chaves que consegue identificar um determinado conjunto de informações (registro). O banco de dados estruturado ele pode ser dividido em várias tabelas e pode estar em um ou vários locais físicos diferentes como é o caso de gerenciadores de banco de dados que permitem fazer réplicas de suas bases de dados em diferentes servidores.

A lei trata sobre o titular, sendo o proprietário dos dados, pessoa natural ou por pessoa jurídica de direito público ou privado. Através dessa pessoa poderá ser extraídos vários atributos que são dados sensíveis ou não.

Tem-se três tipos de profissionais que são responsáveis pelos dados de uma empresa sendo ela pública ou privada que são o controlador, sendo ela uma pessoa natural ou jurídica que lhe compete as decisões referentes ao tratamento do dado. Responsável por definir o tipo de tratamento que será feito com o dado.

O Operador é a pessoa encarregada de direito público ou privado que realiza o tratamento dos dados pessoais em nome do controlador. Ela irá trabalhar os dados para diversos fins, como por exemplo em curso de ensino superior, quais os alunos tiveram melhor ou pior rendimento. Sendo que um determinado aluno poderá não querer que sua nota seja divulgada de forma pública.

O Encarregado, sendo a pessoa indicada pelo controlador irá realizar a comunicação entre o titular, o controlador e a Agência Nacional de Proteção de Dados (ANPD), instituída pela LEI Nº 13.853, DE 8 DE JULHO DE 2019 em seu artigo 55-A, sendo órgão da administração pública federal, integrante da Presidência da República. Uma de suas funções é zelar pela proteção dos dados pessoais, nos termos da legislação, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade. Que poderá adotar medidas de políticas de privacidade dos pessoais como políticas internas e adotar técnicas como criptografia.

Para lei conforme o art. 5 inciso X, tratamento são: “todas as operações que podem ser realizadas com os dados pessoais, tais como produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferências, difusão e extração”.

Há diversas operações que podem ser realizadas com os dados, como por exemplo a produção de dados, com os dispositivos eletrônicos que tem como é o caso do celular que possui interação com antenas em diversas tecnologias de conexão, tais como *bluetooth*, *wireless*, *2G*, *3G*, *4G*, podem produzir dados de forma diversas, como por exemplo a localização de uma pessoa pelo celular.

O desrespeito da legislação vigente os agentes públicos que assumirem as funções de controlador, encarregado e operador, poderão responder por ato de improbidade administrativa em seu artigo 11 da lei 8.429/1992, por esse fato deve se preparar para atender a nova legislação.

Vários incidentes podem ocorrer com os equipamentos e software que são armazenados os dados digitais. Um exemplo é o sítio intitulado “;--have i been pwned ?”<sup>4</sup>, o qual permite saber se o seu e-mail já esteve exposto na internet pelo fato de falha de segurança em algum site que realizou o cadastro e quais os dados pessoais foram expostos.

Para realizar a consulta, o usuário digita o seu e-mail e o site mostra quais os sítios da internet tiveram incidentes e os dados dos seus usuários foram compartilhados na internet. Como foi caso de uma importante rede social de curriculum que teve em 2016, 164 milhões de endereços de e-mail e senhas expostos. Conforme informação do site foi invadido em 2012. Sendo que os dados comprometidos foram e-mail e senha. Caso os proprietários utilizarem outros serviços com esse endereço de e-mail e senha podem ter sido invadidos por hackers.

<sup>4</sup> <https://haveibeenpwned.com/> acessado em 02/07/2020

Muitas vezes pessoas recebem e-mail de desconhecidos e uma das hipóteses são por causa da falha de segurança de alguns desses sites e o atacante conseguiu essa informação. Muitas vezes captam até uma senha utilizada nesse sitio invadido que poderá ser utilizada em outro sitio.

Uma importante empresa de software em outubro de 2013, teve 153 milhões de contas foram violadas, cada uma contendo um identificador interno, nome de usuário, e-mail, senha criptografada e uma dica de senha em texto sem formatação. A criptografia da senha foi mal executada e o algoritmo de segurança foi descoberto, decifrando a senha dos usuários. As dicas não criptografadas também revelaram muito sobre as senhas, aumentando ainda mais o risco que centenas de milhões de clientes. Os dados comprometidos foram: endereços de e-mail, dicas de senha, senhas, nomes de usuário.

As atividades de tratamento de dados pessoais conforme a lei de proteção de dados em seu art. 6 deve-se observar os seguintes princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não-discriminação, responsabilização e prestação de contas.

## **5. Conclusões**

A Lei Geral de Proteção de Dados, trouxe uma regulamentação sobre o tratamento dos dados pessoais sensíveis, o que antes somente havia princípios éticos sobre o tratamento de dados sensíveis, agora existe uma legislação que indica o que pode ser feito com tais dados e visa informar o cidadão referente com os seus dados estão sendo tratados. A Lei de Proteção de Dados recepciona a Lei de Acesso a Informação.

Referente ao agente público, sua função visa atender a Administração Pública que por sua vez através da Lei de Acesso a Informação, os dados devem ser divulgados para atender os princípios constitucionais de publicidade, sendo que a população tem o direito de saber como o direito público está sendo gasto e que informações sensíveis tais como nome do agente público e seus rendimentos, não ferem o princípio da privacidade do agente público.

O agente público que estiver na função de controlador, encarregado de dados, terá um importante papel no tratamento das informações para respeitar a Lei de Acesso a Informação e a Lei de Proteção de Dados para garantir o respeito a legalidade e não incorrer em improbidade administrativa por falta de zelo pelos dados públicos.

A Sociedade da Informação com a Lei de Acesso a Informação propicia o controle social, sendo que qualquer cidadão poderá ter acesso a dados públicos e questionar sobre seus

gastos e verificar qualquer tipo de mal feito o qual poderá fazer sua denúncia de forma anônima ou identificada através dos sítios da administração pública.

Referente as perguntas realizadas durante o artigo, mesmo os dados sendo consideráveis sensíveis do agente público o qual temos um aparente conflito constitucional entre privacidade e publicidade, os dados dos agentes públicos podem ser divulgados pelo fato que estão prestando um serviço público e sendo uma informação de interesse geral e referente aos sua remuneração, também podem ser publicados pelo fato que estão sendo pagos com dinheiro público e o interesse público ele é mais importante que o interesse privado.

Porém os dados que não são necessários para os atos públicos, a Administração Pública terá que atender os requisitos da LGPD, como por exemplo cifrar as informações dos agentes públicos em suas bases de dados que não tenham interesse a população respeitando o princípio da privacidade.

O princípio da publicidade não fere o princípio da privacidade do agente público como muito bem interpretado pelo Douto Ministro Carlos Ayres Britto do Superior Tribunal Federal, que fundamentou o julgado de Repercussão Geral nº 483, que não há conflito entre o princípio da publicidade com o princípio da privacidade dos dados do agente público pelo fato do agente público estar prestando um serviço público sendo de interesse de todos o investimento do dinheiro público, referente aos seus rendimentos.

Com a LAI, e com a divulgação dos dados públicos está sendo propiciado o controle social que propicia a qualquer cidadão verificar onde está sendo empregado o dinheiro público, bastando para isso acessar o site da Transparência Pública, porém para criticar os dados se faz necessário conhecimento técnico sobre o assunto que está sendo estudado.

## **REFERÊNCIAS**

ARAS NETO, José Soares Ferreira, Direito Administrativo sintetizado, 3. ed., Rio de Janeiro: Forense; São Paulo: MÉTODO, 2019.

BÉO, Cintia Regina, Controle da Administração Pública, Coordenação Eloísa Machado, São Paulo, FGV Direito, SP, 2014, pag. 39-61.

GOMES, Luiz Manoel Junior, Lei de Improbidade Administrativa: obstáculos à plena efetividade do combate aos atos de improbidade, Brasília, Conselho Nacional de Justiça, 2015.

DI PIETRO, Maria Sylvia Zanella. Direito Administrativo, 23ª Edição, São Paulo, Editora Atlas, 2010 p. 71.



GONÇALVES, Tânia Carolina Nunes Machado. Gestão de Dados Pessoais e Sensíveis pela Administração Pública Federal: desafios, modelos e principais impactos com a nova Lei, Dissertação (Mestrado em Direito) – Centro Universitário de Brasília (UnICEUB), 2019. Brasília, 2019. p. 147.

FAZZIO, Júnior Waldo, Improbidade administrativa: doutrina, legislação e jurisprudência, 4º ed. Ver. Atual e ampl, São Paulo, Atlas, 2016.

GASPARINI, Diógenes, Direito Administrativo, 17. Ed. atualizada por Fabrício Motta, São Paulo, Saraiva, 2012.

MEIRELLES, Hely Lopes, Direito Administrativo brasileiro, 22. Ed. São Paulo, Malheiros, 1997, P. 72-74.

MORAES, Alexandre de, Direito Constitucional, 18º ed, São Paulo, Atlas, 2005

NEVES, Daniel Amorim Assumpção; Oliveira, Rafael Carvalho Rezende, Manual de Improbidade Administrativa, 4º ed. Ver. Atual e ampl. Rio de Janeiro, Forense, São Paulo, Método, 2016.

REZENDE, Luciano dos Santos, O Regime de Emprego no âmbito da Administração Pública, Revista CEJ, Brasília, Ano XIV, n.51 p. 76-84 out./dez 2010.

SILBERSCHATZ, Abrahan; KORTH, Henry, F., Sistemas de banco de dados, tradução de Daniel Vieira, Rio de Janeiro, Elsevier, 2006

SILVA, De Plácido e, Vocabulário Jurídico / atualizações: Nagib Slaibi Filho e Gláucia, Rio de Janeiro, 2004.

**Fretz Sievers Junior**

Graduado em Engenharia da Computação

Bacharel em Direito pela Universidade Braz Cubas

Ciências Contábeis pela Universidade da Cidade de São Paulo

Mestrado em Engenharia Eletrônica e Computação pelo Instituto Tecnológico de Aeronáutica

Mestrando em Direito PUC/SP

Doutorado em Engenharia Eletrônica e Computação pelo Instituto Tecnológico de Aeronáutica

Atualmente é Professor de Ensino Superior da Faculdade de Tecnologia Mogi das Cruzes, Faculdade de

Tecnologia de Mauá, Universidade Mogi das Cruzes (UMC)

fretz@uol.com.br