FACULDADE DE TECNOLOGIA DE AMERICANA
"MINISTRO RALPH BIASI"

Curso de Tecnologia em Segurança da Informação

Augusto Silvério de Araújo Leandro
Gustavo Henrique de Andrade

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E A LGPD

Americana, SP
2021

FACULDADE DE TECNOLOGIA DE AMERICANA
"MINISTRO RALPH BIASI"

Curso de Tecnologia em Segurança da Informação

Augusto Silvério de Araújo Leandro
Gustavo Henrique de Andrade

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E A LGPD

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Dr. Daives Arakem Bergamasco.

Área de concentração: políticas de segurança da informação.

Americana, SP

2021

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

L475p LEANDRO, Augusto Silvério de Araújo

Política de segurança da informação e a LGPD. / Augusto Silvério de Araújo Leandro, Gustavo Henrique de Andrade – Americana, 2021.

47f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Dr. Daives Arakem Bergamasco

1 Segurança em sistemas de informação I. ANDRADE, Gustavo Henrique de II. BERGAMASCO, Daives Arakem III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Augusto Silvério de Araújo Leandro
Gustavo Henrique de Andrade

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E A LGPD

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: políticas de segurança da informação.

Americana,29 de Junho de 2021.

Banca Examinadora:

Daives Arakem Bergamasco
Doutor
Fatec Americana

Marcus Vinicius Lahr Giraldi
Especialista
Fatec Americana

Diogenes de Oliveira
Mestre
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar gostaríamos de agradecer o nosso orientador Daives Arakem Bergamasco, que nos acompanhou e auxiliou no desenvolvimento do nosso TCC e esteve presente em todos os momentos, quando solicitado; Outra pessoa que foi fundamental no desenvolvimento do nosso tema e base para a pesquisa, foi a Juliane Borsato, onde compartilhou várias bases de de informação e fóruns, para o desenvolvimento da pesquisa.

Dedicamos este trabalho a todos que nos ajudaram, a todos os professores do curso de Segurança da Informação que nos apoiaram durante essa jornada, que apoiaram nos momentos bons e nos mais difíceis, impedindo de nos fazer desistir durante o percurso. E agradecemos também a todos amigos e familiares que contribuíram com a realização deste projeto.

RESUMO

A presente pesquisa objetivou fomentar reflexões acerca da política de segurança da informação e a lei geral de proteção de dados ou LGPD, sendo esta uma lei que está em vigor desde o segundo semestre de 2020, cabendo a todas as pessoas a priori estar cumprindo a lei ao seu rigor. De tal modo, a proposta desta pesquisa será evidenciar como essa lei impacta a rotina das empresas. De tal modo, o problema proposto para esta pesquisa partiu do seguinte questionamento: qual a importância da política de segurança da informação e a Lei Geral de Proteção de Dados no âmbito das organizações? A partir do exposto, o objetivo geral desta pesquisa foi tratar sobre a importância da Lei Geral de Proteção de Dados Pessoais. No que tange à metodologia, o trabalho desenvolvido foi baseado em pesquisas bibliográficas, artigos e livros que abordam o tema da LGPD e segurança da informação, apoiando-se em revistas e jornais, periódicos. O material de pesquisa foi o resultado de busca e estudo de informações em livros de referência e artigos acadêmicos. Quanto aos descritores utilizados, a pesquisa utilizará as seguintes palavras-chaves para realização de busca: segurança, informação e LGPD. Já no que diz respeito ao período dos artigos e trabalhos publicados, foi estabelecido o período de 10 anos para delimitação, sendo que os autores renomados da área, não se definiu um período específico. Dentre as principais considerações obtidas com a pesquisa é possível ressaltar que o objetivo da LGPD não é acabar com nenhum tipo de mercado, mas apenas coibir práticas abusivas. Então, se o negócio depende do compartilhamento de dados, é importante às empresas irem se ajustando, adequando à política de proteção de dados, conforme a lei exige, é importante ir colhendo o consentimento do cliente, afinal, nenhum cliente gostaria de ter os seus dados invadidos.

Palavras Chave: proteção; dados; empresas.

ABSTRACT

This research aimed to foster reflections about the information security policy and the general data protection law or LGPD, which is a law that has been in force since the second half of 2020, and it is up to all people to comply with the law to its rigor. In such a way, the purpose of this research will be to evidence how this law impacts the companies' routine. In such a way, the problem proposed for this research started from the following question: what is the importance of the information security policy and the General Data Protection Law within the scope of organizations? Based on the above, the general objective of this research was to address the importance of the General Law for the Protection of Personal Data. Regarding the methodology, the work developed was based on bibliographic research, articles and books that address the LGPD and information security theme, supported by magazines, newspapers, and periodicals. The research material was the result of searching and studying information in reference books and academic articles. As for the descriptors used, the research will use the following keywords to perform the search: security, information, and LGPD. Regarding the period of articles and published works, the 10-year delimitation period was established, and the renowned authors in the area did not define a specific period. Among the main considerations obtained with the research, it is possible to emphasize that the objective of the LGPD is not to end any type of market, but only to prevent abusive practices. So, if the business depends on data sharing, it is important for companies to adjust, adapting to the data protection policy, as required by law. It is important to collect the consent of the client, after all, no client would like to have their hacked data.

Keywords: *protection; personal data; companies.*

1 INTRODUÇÃO

Os avanços tecnológicos das últimas décadas causaram forte impacto na ciência do direito, fazendo inclusive surgir lacunas, isto é, problemas jurídicos sem uma solução aparente. Percebe-se que muitos indivíduos não seriam capazes de cometer delitos nas relações concretas (indivíduo x indivíduo) e encontram no mundo virtual certa segurança para o cometimento destes, como por exemplo, o estelionato, tráfico de drogas, invasão de privacidade, dentre outros.

A LGPD ou Lei Geral de Proteção de Dados é uma lei que está em vigor desde o segundo semestre de 2020, cabendo a todas as pessoas a priori estar cumprindo a lei ao seu rigor. De tal modo, a proposta desta pesquisa será evidenciar como essa lei impactará a rotina das empresas, ressaltando quais os impactos que ela tende a trazer para estas, tendo em vista que os dados pessoais são a grande riqueza digital, por essa razão é importante protegê-los.

No mundo da administração de empresas muitos são os dados pessoais envolvidos nos processos, dados estes que deveriam respeitar indistintamente a lei, todavia, nos fluxos de trabalhos nos escritórios todo cuidado é pouco. Esse cuidado deve iniciar desde o momento da recepção, da análise do fluxo de dados dentro do escritório, no ambiente de trabalho, isso é muito importante para que seja possível saber nas mãos de quem estão os dados, se estão realmente de posse das pessoas que vão trabalhar com estes dados, se há algum dado fora de acessibilidade, dados nos meios computacionais.

A partir desses preceitos, esta pesquisa se justifica pelo fato de que estudar a importância da política de segurança da informação e a Lei Geral de Proteção de Dados – LGPD no âmbito das organizações torna-se imprescindível no cenário organizacional na atualidade, pois vivencia-se um cenário cada vez mais competitivo, no qual as empresas precisam que suas atividades sejam feitas conforme as metas estabelecidas, pautadas pelas legislações vigentes.

Nesse sentido, é preciso certificar se esses dados estejam bem protegidos e fora do alcance das pessoas que não precisam desses dados. Assim, é possível evidenciar que a LGPD é a melhor resposta geral para cobrir a proteção da individualidade das pessoas e das empresas nesse serviço.

No que tange ao problema proposto para esta pesquisa, ela partiu do seguinte

questionamento: qual a importância da política de segurança da informação e a Lei Geral de Proteção de Dados no âmbito das organizações?

A partir do exposto, o objetivo geral desta pesquisa foi tratar sobre a importância da Lei Geral de Proteção de Dados Pessoais. Todavia, antes de entrar propriamente nesta lei, a pesquisa tratou de algumas noções introdutórias sobre o tema da proteção de dados pessoais no Brasil.

Como objetivos específicos têm-se: conceituar privacidade e proteção de dados pessoais e as legislações vigentes; destacar os principais aspectos da Lei Geral de Proteção de Dados, além de discutir a importância da segurança de dados para as organizações.

Todavia, é importante explicitar que as contribuições fomentadas por esta pesquisa são de natureza acadêmica, mas, sobretudo, de natureza social, pois a mesma visa ofertar informações necessárias ao público-alvo acerca da importância desta legislação no âmbito das organizações.

2 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Ao refletir sobre a privacidade e proteção de dados pessoais, convém, primeiramente, assinalar o conceito de dados pessoais. Esse conceito é dado pelo art. 5º da Lei 13.709/18, a Lei Geral de Proteção de Dados, que considera dado pessoal como toda a informação que torna a pessoa identificada ou identificável (BRASIL, 2018). Ou seja, é toda informação que permite saber quem é aquela pessoa, e esse dado é relacionado somente à pessoa natural, ou seja, a pessoa física. São somente as pessoas humanas, ele é um atributo humano.

As pessoas jurídicas não têm dados pessoais e, portanto, a lei não protege os dados dessa pessoa jurídica, apenas os dados pessoais das pessoas físicas relacionadas a essas pessoas jurídicas. Assim, sobre a proteção de dados pessoais, Doneda (2006) assinala que:

> Embora a proteção dos dados pessoais derive da tutela da privacidade, aquela não se restringe a esta, por isso é necessário compreendê-la (proteção dos dados pessoais) e argumentar pela sua defesa com base em outras garantias fundamentais, como, por exemplo, o direito à liberdade e à defesa da autonomia privada (DONEDA, 2006, p. 356).

O artigo 5º da referida Lei (2018) traz também outros conceitos, como o conceito de dados, conceitos correlatos à própria lei. Um deles é o conceito de dados pessoais sensíveis. Esses dados são aqueles que expõem mais as pessoas, são dados muitas vezes relacionados à intimidade do cidadão, e por isso ele demanda uma proteção maior. Nas palavras de Tepedino (2001) *apud* Tomizawa (2008, p. 107):

> A utilização de dados pessoais pelos bancos de dados, em especial os chamados “dados sensíveis”, que envolvem histórico de saúde, orientação religiosa, opção sexual, histórico policial, etc., possibilita a descoberta de aspectos relevantes da intimidade dos cidadãos.

Exemplos desses dados são aqueles relacionados à orientação sexual, à origem racial, à orientação política. Por esses dados muitas vezes levarem algum tipo de discriminação ou preconceito, a lei cria uma proteção e cria requisitos mais rígidos para que se possa coletar e tratar esses dados.

Raminelli e Rodegheri (2016) destacam sobre a importância da proteção de dados no ambiente online:

> [...] o grande desafio que se coloca à frente dos cidadãos é o controle dos dados pessoais que pode ser feito por empresas ou, até mesmo, pelos

> governos. Há possibilidade de verificação, por meio de um monitoramento online, de preferências artísticas, musicais, hábitos de vida, de viagens, operações financeiras, orientação sexual, crenças religiosas, entre outros.(RAMINELLI; RODEGHERI, 2016, p. 92).

Outro conceito dado também pelo artigo 5º é o conceito de dado anonimizado. Esse dado não é pessoal. A lei não considera ele como um dado pessoal porque ele não permite identificar a pessoa que forneceu este dado. Na realidade, a pessoa pode se identificar, mas esse dado será ocultado em seguida ou ele sequer é coletado com a identificação da pessoa (BRASIL, 2018).

Leonardi (2012, p. 79) assinala que “a importância da internet para a valorização dessa perspectiva da privacidade é evidente e leva a uma busca necessária de novos conceitos de proteção da esfera privada”.

De tal modo, o conceito de privacidade no atual contexto da tecnologia está inserido na definição da proteção de dados, que vai além da tutela da intimidade individual, pois se encontra vinculada à legalidade da ação pública.

Exemplificando, é o que acontece com os institutos de pesquisa. Esses institutos vão às ruas e perguntar às pessoas qual a religião delas, em quem elas vão votar sem que isso permita a identificação dessa pessoa. Apenas com a finalidade de criar um perfil geral daquela localidade. Conforme Doneda (2006):

> O termo é específico o suficiente para distinguir-se de outras locuções com as quais eventualmente deve medir-se, como a imagem, honra ou a identidade pessoal; e também é claro o bastante para especificar seu conteúdo, um efeito da sua atualidade. Mas esta escolha não é consequência somente das fragilidades das demais opções: ao contrário, ela revela-se por si só a mais adequada, justamente por unificar os valores expressos pelos termos intimidade e vida privada (DONEDA, 2006, p. 356).

O conceito de dado pessoal, sensível ou não, já deixa claro a importância de se proteger esses dados. Eles são direitos fundamentais da pessoa, muitas vezes relacionados à liberdade, à intimidade, à privacidade em si. Por isso a lei se torna fundamental, por isso essa lei foi criada inclusive porque os dados pessoais são a grande riqueza e uma riqueza que pertence ao indivíduo.

2.1 LEGISLAÇÕES DE PROTEÇÃO DE DADOS PESSOAIS

Como é sabido, a tecnologia está em processo de avanço o tempo todo, com isso, levando também os crimes entrarem cada vez mais nesse mundo tecnológico.

Assim, o Direito se viu no dever de regular as relações que passaram a ser desenvolvidas no ambiente virtual.

A liberdade de acesso de informação fez surgir entre os especialistas, duas palavras-chave: intenção e comportamento, o que os fez questionar qual seria o comportamento de uma pessoa diante sua intenção naquele ambiente. Foi percebido, portanto, que a partir do momento em que um indivíduo tem boas intenções para obter informações no ambiente cibernético seu comportamento é um. No entanto, a partir do momento que a intenção é usufruir de alguma forma e ter alguns comportamentos não convencionais, não sociais, isso começa a se tornar uma nova preocupação a nível jurídico.

Sob esta ótica, para tratar da proteção de dados pessoais no Brasil, antes de mais nada, é importante explicitar que a tutela da privacidade se encontra prevista na legislação brasileira na Constituição Federal de 1988 que protegem tanto no art. 5º, inciso 10º, segundo a CF/1988 e no Código Civil (2002). Todavia, Filho (2005) ressalta que:

> Na falta de um conjunto amplo e concatenado de leis protetivas da privacidade, em suas mais variadas manifestações, o instrumento do jurista no trato desses assuntos será inevitavelmente a Constituição Federal, onde estão assentes os princípios basilares desse direito personalíssimo. Acontece que a Constituição, apesar de conter espalhados em vários dispositivos garantias relacionadas com o “direito à privacidade”, não fornece meios seguros para definir sua extensão e alcance.

No que tange ao Código Civil (2002) o art. 21 do Código Civil trata da intimidade à vida privada e a honra e imagem das pessoas considerando que esses direitos são invioláveis. Ainda nas palavras de Filho (2005, p. 13): “O novo Código Civil se limitou a expressar que “a vida privada é inviolável”, podendo o Juiz adotar as medidas necessárias para protegê-la (art. 21)”.

Todavia, embora já houvesse uma previsão expressa no ordenamento jurídico quanto à garantia desses direitos passou-se a considerar que necessitava uma proteção especial. Conforme Pereira (2006, p. 241): ainda que uma empresa “que possua seu sistema informático interconectado à Rede possa estar mais propensa a sofrer um ataque hacking, indiretamente, a privacidade das pessoas, vale dizer, dos internautas, encontra-se em perigo”.

Isso se deve ao fato de que com o desenvolvimento da economia e vivendo no que se chama atualmente de sociedade da informação, a exposição dos dados pessoais passou a ser ainda maior do que antes. É muito comum se deparar com

episódios de vazamento de dados, por exemplo, vazamento de senhas ou até mesmo documentos das pessoas, o que gera uma série de consequências.

> Por tal razão, já há algum tempo, não apenas os juristas, mas a própria sociedade, por meio de representantes lúcidos do que se costumou chamar "sociedade civil", deram-se conta do risco representado pelo potencial maléfico dos bancos de dados de caráter pessoal, a ponto de criticar seu uso indiscriminado e pugnar pelo controle de seu funcionamento, com a imposição de regras claras para o seu uso transparente (CASTRO, 2002, p. 41).

Então, mundialmente passou-se a haver uma preocupação cada vez maior de que a proteção dos dados pessoais fosse tutelada por uma legislação específica na sociedade em que se vive hoje em dia, em que os dados são praticamente equiparados a mercadorias.

Por outro lado, era muito importante que ao mesmo tempo em que se protegesse esses dados pessoais do indivíduo, também não se cercear a liberdade de expressão das pessoas, daí a necessidade de se desenvolver uma legislação compatível com o tempo.

De tal modo, no Brasil, é possível citar alguns marcos normativos. O primeiro deles, que não trata exatamente sobre proteção de dados pessoais, é a Lei do Cadastro Positivo, a Lei 12.414/2011, mas que vale a menção porque é uma lei que prevê a respeito dos dados pessoais sensíveis.

Após o período de 3 anos, depois de muita discussão da sociedade, surge um marco civil da internet, a Lei 12.965/2014 trazendo diversas disposições sobre a utilização da internet no Brasil.

Conforme Santos e Júnior (2018, p. 04): o Marco Civil da Internet se trata de "uma norma basicamente principiológica, a garantia da liberdade de expressão, a garantia da neutralidade da rede e a proteção à privacidade do usuário, passa-se a análise de cada um deles".

A partir desses preceitos, é possível destacar o princípio que diz respeito à proteção dos dados pessoais, sendo que no art. 3º estabelece-se como um dos princípios da utilização da internet no Brasil, a proteção da privacidade e também a proteção dos dados pessoais, na forma da lei.

Ou seja, embora o marco civil assegura a proteção, ele releva para uma lei específica que faça uma regulamentação adequada do tema. E também vale mencionar o Decreto 8.771/2016 que regulamenta o marco civil.

A respeito de algumas das disposições específicas do marco civil, ainda nesse período em que ele ficou em vigência até hoje essas disposições também continuam a valer sobre a proteção de dados pessoais.

A primeira delas diz respeito à aplicabilidade da legislação brasileira no tema de proteção à privacidade de dados. Ou seja, toda vez que houver operações de coleta, armazenamento, guarda, tratamento de registros que envolvam dados pessoais a legislação Brasileira deve ser aplicada desde que qualquer dessas operações mencionadas ocorra em território nacional; pelo menos um dos terminais estejam localizados no Brasil (terminal é aquele equipamento que esteja conectado à rede , realizando uma dessas operações).

E, por último, quando houver oferta de serviço a público Brasileiro ou pelo menos um integrante do grupo econômico que realiza essas operações possua esse estabelecimento no Brasil.

Dessa forma ficou bastante abrangente a aplicabilidade da lei Brasileira no que refere à proteção de dados na utilização da internet.

O marco civil traz também direitos e garantias do usuário, salientando-se aqueles que dizem respeito à proteção de dados. Então, é possível citar:

> (...) a inviolabilidade da intimidade da vida privada, a inviolabilidade do fluxo das comunicações pela internet, a inviolabilidade do sigilo das comunicações privadas armazenadas e também a proteção e o direito à informações claras e completas sobre coleta, uso armazenamento, tratamento e proteção de dados pessoais que só podem ser utilizada para finalidades que justifiquem a sua coleta.

Ou seja, não é possível coletar, realizar tratamento de um dado pessoal sem que isso tenha uma finalidade clara, um destino específico ou que não sejam vedadas pela legislação e ainda que estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicação de internet.

O marco civil estabelece também que é obrigatório o consentimento expresso sobre a coleta, o armazenamento e o tratamento de dados pessoais (BRASIL, 2014). O usuário, aquela pessoa que está cedendo os dados, deve dar o consentimento expresso, e esse consentimento tem que ser destacado das demais cláusulas contratuais. Não é possível haver uma cláusula em que, dentre outros assuntos, também trata do consentimento. O consentimento tem que estar bastante claro e para isso, exige-se até mesmo que ele seja uma cláusula separada de todas as outras.

E, por fim, o marco civil (2014) prevê também o direito à exclusão definitiva desses dados pessoais que foram fornecidos pelo usuário quando o usuário requerer que esses dados sejam excluídos ao término da relação entre as partes, com exceção das hipóteses em que é obrigatório por lei que essa guarda seja realizada, seja pelo que consta do próprio marco civil ou ainda na Lei Geral de Proteção de Dados.

2.2. GUARDA E DISPONIBILIZAÇÃO

No que tange à guarda e disponibilização, o marco civil da internet estabelece que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações devem preservar a intimidade, vida privada e imagem das partes envolvidas (BRASIL, 2014). Deste modo, cumpre assinalar que o ordenamento jurídico brasileiro adota o modelo de retenção que é contrário ao modelo de preservação de dados.

Isso significa que a lei obriga que os provedores guardem por determinado período os registros ao passo em que o modelo de preservação determina que os registros só deveriam ser guardados a partir do momento em que houvesse uma ordem específica para isso. Assim sendo, a segurança de informação se faz necessária pelos seguintes motivos:

> A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado. [...] a função da segurança da informação é viabilizar os negócios [...] (ABNT, 2005, p. 02).

A disponibilização pelo provedor dos dados pessoais que ele guarda somente pode ocorrer com ordem judicial. Então, não pode ocorrer do provedor disponibilizar dados pessoais simplesmente ao mero requerimento do interessado, a não ser que seja a própria pessoa. Do contrário, ele só vai poder disponibilizar dados pessoais de terceiros com ordem judicial.

Todavia, há uma exceção; os dados considerados meramente cadastrais são aqueles dados que são fornecidos ao se realizar alguma compra ou acessar um aplicativo, o que implica em dados como nome, endereço, filiação, etc. Esses são considerados dados meramente cadastrais, e nesse caso esses dados podem ser

solicitados diretamente por autoridades administrativas que tenham competência legal para efetuar essa requisição, na forma da lei.

Neste tocante, Reinaldo Demócrito Filho afirma que:

> (...) se, por um lado, a coleta de informações pessoais pode favorecer negócios, facilitar decisões governamentais ou mesmo melhorar a qualidade de vida material da sociedade como um todo, outros valores necessitam ser considerados à luz da privacidade individual (FILHO, 2005, p. 103).

Conforme o autor, é importante observarmos que tais práticas podem ser consideradas um problema sócio-jurídico, haja vista ser necessário delimitar as formas em que serão exercidas a coleta dessas informações a fim de que seja preservada a privacidade que todo indivíduo possui.

Ou seja, em casos que a lei determine que a autoridade administrativa possa fazer essa solicitação porque do contrário ela também não poderá ter acesso.

A partir daí, essas exigências e obrigação dos provedores se descumprida por eles pode levar à imposição de sanções que podem ser muito graves, desde uma advertência e uma multa ou até mesmo a suspensão ou proibição de sua atividade. Então, de forma alguma o provedor poderá fornecer dados pessoais sem que seja por ordem judicial (CASTRO, 2002).

Outra situação importante de distinguir se dá na diferença dos dados cadastrais, dados de conexão e interceptação de conteúdo. Os dados cadastrais, como explicitado, são os dados fornecidos pelo usuário para acessar determinados serviços. Ou seja, são os dados mais simples e corriqueiros que a pessoa mesmo irá inserir ali para que ela tenha acesso a determinado serviço.

Já os registros de conexão têm a sua definição no próprio marco civil da internet, em seu art. 5º inciso 6º e seria o conjunto de informações que diz respeito àquela conexão que o usuário efetuou, onde vai terá que constar a data e hora em que ele iniciou a conexão e que ele terminou a conexão, com o tempo total de duração e também o endereço de ip utilizado (BRASIL, 2014).

Ou seja, esse registro de conexão que é o que deve ser guardado pelo provedor é o que só pode ser também fornecido mediante ordem judicial e que vai servir em alguns casos, por exemplo, para tentar identificar a pessoa que realizou determinada conexão (JORGE e WENDT, 2013).

O registro de acesso é bastante parecido. Trata-se do conjunto de informações

referentes à data e hora do uso de uma determinada aplicação da internet, a partir de um determinado endereço de ip (art. 5º, VIII, Marco Civil).

Portanto, o registro de acesso não se trata da conexão de todo o tempo em que a pessoa ficou utilizando, mas o acesso específico a determinada aplicação na internet, como determinado site ou aplicativo, por exemplo.

Por esta via, cabe também diferenciar os dados cadastrais, os dados de conexão que são somente esses dados que se referem ao período basicamente em que a pessoa utilizou o endereço de ip da interceptação de conteúdo. Quando se diz que os provedores têm essa obrigação de guarda não diz respeito à interceptação de conteúdo, que seria propriamente o teor da comunicação em si, o que aquela pessoa conversou, o que ela está falando, o que ela está escrevendo.

Essa interceptação de conteúdo só pode ocorrer em hipótese também por ordem judicial, mas muito mais restritas que seria aí uma garantia até mesmo constitucional, somente para fins de investigação criminal ou instrução processual penal (JORGE e WENDT, 2013).

Então, ao se dizer que os provedores têm o dever de realizar a guarda dos dados de conexão, isso se refere somente a esses dados que possibilitam identificar o usuário, o que ele acessou e durante qual o período, e não identificar o teor, o conteúdo da comunicação que ele realizou porque nesse caso o acesso é muito mais restrito do que nas situações anteriores que podem ser utilizadas para as mais diversas situações.

A guarda dos registros de conexão deve ocorrer pelo prazo de um ano, ela deve ser sigilosa, tanto assim que a lei determina que o provedor de conexão não pode nem mesmo transferir essa responsabilidade pela manutenção a terceiros. Esse prazo de um ano também pode ser estabelecido, ou seja, ele pode ser aumentado, desde que tenha pedido da autoridade policial ou alguma outra autoridade administrativa ou do Ministério Público (BRASIL, 2014).

Mas isso não significa que automaticamente ao fazer esse pedido de que guarde por mais tempo os registros, ele vai ter acesso. Então, a autoridade do ministério público pode se dirigir diretamente ao provedor e requerer que o prazo seja abastecido, porém ele deve ingressar judicialmente para que esses dados sejam disponibilizados. Nesse sentido, Jorge e Went (2013) explicitam:

> Outra circunstância que poderá derivar da análise dos documentos é

> a solicitação ao Poder Judiciário para que determine ao administrador de rede de determinado local que preste informações específicas e técnicas que visem indicar diretamente a máquina de onde partiu o acesso. Em regra, tal circunstância ocorre quando nos deparamos com redes corporativas. Essa determinação judicial poderá ser encaminhada ao administrador de redes para cumprimento ou entregue pessoalmente por autoridade policial ou oficial de justiça. Esta última medida é fundamental em casos em que se suspeita quanto ao processo de administração da rede ou do próprio administrador ou sua equipe (JORGE & WENDT, 2013, p. 52-53).

E ainda é vedado que os provedores de conexão guardem os registros de acesso a aplicações de internet. Os provedores de conexão devem guardar somente os dados da conexão e não de acesso específico à aplicações de internet. Essa já seria a responsabilidade dos provedores de aplicação, pois esses provedores vão ter o dever de guardar esse tipo de registro que são os registros de acesso.

Nesse caso, todavia, a obrigatoriedade, ela existe somente para a pessoa jurídica que exerce atividade de forma organizada profissionalmente e com fins econômicos". Assim, essas pessoas vão ter o dever de guardar esses registros e acesso de aplicações pelo prazo de seis meses. Em outros casos vai depender de determinação judicial que vai analisar o caso concreto para determinar o período em que os dados devem ser guardados.

Da mesma forma dos outros provedores de conexão, essa guarda deve ser sigilosa e somente poderá ser disponibilizada com autorização judicial. Também como no outro caso, esse prazo pode ser aumentado a pedido da autoridade policial administrativa, do Ministério Público. Porém, o mero pedido de elasticidade em seu prazo não dá direito ao acesso, então o acesso sempre vai ser mediante ordem judicial.

> A comunicação entre pessoas, feita de forma privada por qualquer meio (através de correspondência postal, telegráfica, por meios informáticos ou por telefone), envolve a transferência entre elas de informações pessoais e, por isso, não pode ser invadida (salvo nos casos previstos na própria Constituição), em atenção à privacidade individual. A garantia constitucional do sigilo das correspondências e troca de informações entre pessoas, feita de forma privada por qualquer meio de comunicação, também delineia os limites e da conformação à privacidade informacional como direito fundamental do cidadão (FILHO, 2005, p. 121).

Para os provedores de acesso a aplicações, eles têm vedação de guardar registro de acesso a outras aplicações de internet, ou seja, eles só podem guardar os registros deles próprios, a não ser que tenha consentimento do próprio usuário, para que seja feita essa guarda de registro ou dados pessoais que sejam excessivos

em relação à finalidade.

Então, os dados pessoais que são requeridos devem ser unicamente aqueles necessários para que o usuário possa se utilizar daquele serviço na internet. Se aquele dado for excessivo, ou seja, estranho àquela relação, ele não deve ser guardado, exceto nas hipóteses previstas pelo próprio marco civil ou nas hipóteses previstas na Lei Geral de Proteção de Dados. Nesse sentido, convém salientar que:

> A bem da verdade, a privacidade não é um fim em si mesma. Reconhecemos sua importância vital para nós porque ela é um instrumento para realização de outros objetivos. O interesse da sociedade em reconhecer valor na privacidade reflete um interesse nos resultados que ela propicia. Alan Westin têm sugerido que a privacidade desempenha um papel essencial na consecução de quatro interesses perfeitamente identificáveis: a) autonomia individual; b) proteção contra exposição pública; c) oportunidade para avaliação e tomada de decisões; e d) limitação e proteção da comunicação (FILHO, 2005, p. 16).

Importa ainda salientar uma lei completamente estranha a essas tratativas, a Lei 13.344, de 2016 que alterou o Código de Processo Penal, trazendo aí também um tipo de dado que merece proteção, que são os dados de localização.

O artigo 13-B dispõe que em alguns casos, também mediante autorização judicial, quando houver interesse na investigação criminal, as empresas prestadoras de serviços de telecomunicações são obrigadas a fornecer os dados de sinais ou informações que permitam a localização da vítima ou de suspeitos de delitos em curso.

É importante atentar para esse dispositivo que ele não diz respeito à autorização para quebra do sigilo das comunicações para que se tenha conhecimento do teor das comunicações, mas meramente que as empresas forneçam dados de localização. Ou seja, uma pessoa está com o celular e de repente a partir dos dados de localização que a empresa fornece é possível verificar em que local estaria a vítima ou até mesmo o suspeito de um crime.

3 PRINCIPAIS ASPECTOS DA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados - LGPD nada mais é do que a Lei Geral de Proteção de Dados. Ela foi sancionada no Brasil em agosto de 2018, e ela teve uma forte inspiração na GDPR – General Data Protection Regulation.

A LGPD tem a função de determinar como as empresas deverão fazer o tratamento de dados dos brasileiros, ou seja, basicamente estabelecer parâmetros de como esses dados devem ser coletados, armazenados, processados e destruídos. O art. 2º da LGPD apresenta um rol de princípio dessa lei, incluindo:

> I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - à inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018, s/p).

Então, basicamente, é preciso saber quem são aqueles que a legislação determina e como ela os conceitua. Nesse sentido, é importante determinar quem é o titular, sendo ele a pessoa natural a que se referem os dados pessoais que são de alguma forma tratados. Importa salientar que a comissão europeia define dados pessoais como:

> Dados pessoais são informações relativas a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa. Dados pessoais que tenham sido descaracterizados, codificados ou pseudônimos, mas que possam ser utilizados para identificar uma pessoa, continuam a ser dados pessoais e são abrangidos pelo âmbito de aplicação do RGPD. Dados pessoais que tenham sido tornados anónimos de modo a que a pessoa não seja ou deixe de ser identificável deixam de ser considerados dados pessoais. Para que os dados sejam verdadeiramente anonimizados, a anonimização tem de ser irreversível (COMISSÃO EUROPEIA, 2020, s/p).

Já o controlador é a pessoa, tanto física ou jurídica, de direito público ou privado que vai tomar as decisões de como devem ser realizados os tratamentos dos dados pessoais. Já o operador também é toda pessoa física ou jurídica, de direito público privado que vai realmente fazer um tratamento desses dados.

O encarregado é o Data Protection Officer que a DPR nominou, ele é o indicado pelo controlador que vai fazer a função de comunicação entre os titulares que vão ter os seus dados processados e o controlador. E também se fala sobre o agente de

tratamento, que nada mais é que o controlador e o operador, segundo a legislação. O tratamento de dados é, portanto, uma conceituação que a legislação trouxe, sendo que ele é basicamente,

> toda operação realizada com dados pessoais que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BONI, 2019, p. 182).

De tal modo, é perceptível que sua conceituação é bastante abrangente, e basicamente na prática se a pessoa tiver acesso de alguma forma aos dados pessoais é bem provável que ela esteja fazendo um tratamento de dados.

A LGPD determina em seu art. 6° os princípios que devem ser seguidos no que tange ao tratamento de dados pessoais:

> I -Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;II -Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;III -Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;IV -Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;V -Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;VI -Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;VII -segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;VIII -prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;IX -Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;X –Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficáciadessas medidas (BRASIL, 2018, s/p).

Outro ponto a se considerar é que referente aos dados que são disponibilizados na internet, nem todos são considerados dados pessoais, basicamente os dados pessoais são aqueles que seja possível identificar ou que seja identificável de alguma pessoa natural.

Então, basicamente, o nome e o cadastro de pessoa física (cpf) pode ser considerado um dado pessoal porque é possível identificar quem é a pessoa. Os dados que permitem que a pessoa seja identificável são aqueles outros dados que não necessariamente podem ser nome, CPF, mas que na soma deles seja possível identificar quem é a pessoa natural titular daqueles dados, portanto, de quem são aqueles dados. Assim, por exemplo, se for possível saber os dados de determinada pessoa, seu endereço, nome da rua, apartamento, etc. basicamente será possível descobrir quem é o titular daqueles dados pessoais (DONEDA, 2017).

A partir dessas considerações, é possível compreender qual seria o primeiro passo das empresas, que basicamente é entender em que formato ela se enquadra perante a lei, e se , de alguma forma, ela está fazendo o tratamento de dados e se esses dados são pessoais ou não.

O segundo passo é se a empresa permite a soberania do titular dos dados. Ou seja, se o titular ou usuário de qualquer serviço, seja online e offline, concede essa soberania sobre os dados coletados. Nesse sentido, as empresas têm que fornecer formas em que seja claro que o titular dos dados tenha dado a anuência para a coleta, armazenamento, transmissão e portanto, que ele anuiu com o tratamento de seus dados (BONI, 2019).

O documento geralmente em que isso está previsto é dentro da política de privacidade ou dentro dos termos de uso, como por exemplo, em caso de startup ou empresa de base tecnológica. É nesse documento que o usuário do serviço, da plataforma vai anunciar de que forma esses dados podem ser tratados.

A legislação então determinou que isso deve ser formalizado em algum documento de forma escrita, não pode ser simplesmente uma anuência verbal. Então, basicamente, a política de privacidade que em alguns casos era implementada dentro do contrato, era somente uma cláusula espaçada dentro de algum contrato ou dentro dos termos de uso, ela tem que ter uma maior relevância (BONI, 2019).

De tal modo, nesse ponto de dar soberania para o usuário titular dos dados, a LGPD vem com as maiores inovações nesse sentido porque essa soberania permite que o usuário possa ter alguns direitos que naturalmente ou anteriormente não era tão claro. Ela permite que o usuário atualmente possa solicitar a alteração dos dados que ele tenha fornecido, que ele possa fazer a revogação, ou seja, que ele recuse a utilização de seus dados e ele pode também pedir a exclusão dos dados que sejam armazenados ou tratados por alguém (BONI, 2019).

De acordo com o Manual da Associação Brasileira de Anunciantes (ABA) para adequação a LGPD, (2019) um programa de boas práticas de governança em privacidade deve:

> a. demonstrar o comprometimento da empresa em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;b. ser aplicável a todo o conjunto de dados pessoais que estejam sob o controle da empresa, independentemente do modo como se realizou sua coleta;c. ser adaptado à estrutura, à escala e ao volume das operações da empresa, bem como à sensibilidade dos dados tratados;d. estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;e. ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f. estar integrado a sua estrutura geral de governança de forma a estabelecer e aplicar mecanismos de supervisão internos e externos;g. contar com planos de resposta a incidentes e remediação; e h. ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas (ABA, 2019, s/p).

Anteriormente, quando o usuário fazia a cessão desses dados, ele não tinha muito como retornar, revogar essa autorização. Hoje em dia a legislação determinou que as empresas têm que permitir que o usuário faça isso, tanto a nível jurídico como no nível tecnológico.

Há ainda que se considerar o nível de amplitude da aplicação da LGPD, sendo possível evidenciar que a LGPD será aplicável a situações de um servidor fora do país ou de uma empresa fora do país. A LGPD determinou as situações em que ela pode ser aplicada, isso é o que se chama de aplicação extra territorial.

Então, a lei explicita que a LGPD vai ser aplicável independentemente do tratamento dos dados ocorrer no país ou fora, e independente do meio, seja dos dados armazenados ou tratados no Brasil ou armazenados ou tratados fora do Brasil. Assim sendo, Rodotà (2008) defende-se a importância da proteção de dados, que conforme o autor, trata-se de uma espécie de direito da personalidade:

> [...] quando os cidadãos passam a ser cada vez mais avaliados e classificados apenas a partir de informações a seu respeito, à proteção e o cuidado com estas informações deixa de ser um aspecto que somente diga respeito às esferas do sigilo ou da privacidade, passando a figurar um componente essencial para determinar o grau de liberdade de autodeterminação individual de cada pessoa (RODOTÀ, 2008, p. 7).

De tal modo, a lei será aplicada desde que o tratamento seja realizado em território brasileiro, então os dados podem ser armazenados fora do Brasil, mas eles

podem ser tratados no Brasil. Ou a atividade de tratamento tenha como objetivo a oferta, o fornecimento de bens e serviços ou o tratamento de dados de indivíduos localizados no Brasil ou se os dados pessoais sejam de alguma forma coletados em solo brasileiro.

Todavia, conforme Boni (2019), a LGPD não trata apenas de dados pessoais, ela dá uma grande relevância sobre dados pessoais, mas ela fala sobre tratamento de dados sejam eles pessoais ou não. Inclusive a lei faz previsões sobre o ponto que se chama de dados anonimizados. A LGPD também não faz previsão somente sobre dados pessoais, ela faz uma previsão de forma ampla sob proteção de dados.

Ainda, em nenhum momento a legislação específica que a LGPD vai ser feita somente para empresas que tenham plataformas digitais, então ainda que seja um escritório de advocacia, um escritório de contabilidade, uma empresa qualquer do ramo tradicional e comum, se a pessoa faz tratamento de dados de acordo com o que a legislação determina, vai ser aplicado a LGPD nesses casos (BONI, 2019).

Outro ponto que a legislação trata é que a partir do momento que se encerra o tratamento de dados, a empresa é obrigada a fazer a exclusão desses dados.

Então, quando a empresa termina de fazer o tratamento de dados de um usuário a partir do que a legislação preceitua, após se encerrar isso a empresa é obrigada a fazer a eliminação desses dados.

3.1. LGPD E ANONIMIZAÇÃO DE DADOS

A LGPD não distingue os dados que não são possíveis de serem armazenados, mas o que pode se chamar de dado pessoal são todos aqueles dados que remetem a um único indivíduo. Por exemplo, para aqueles que trabalham com CPF e CNPJ que são dois dados muito importantes, eles identificam unicamente uma empresa ou um indivíduo (BOFF et al, 2018).

Fora esses dados, os mais comuns são o endereço, estado civil da pessoa e dentro da lei há um conjunto menor ou maior de dados, que são os dados sensíveis, e que dentro da lei são dados que merecem uma atenção muito maior.

Conforme Boff et al (2018), a LGPD trata dos dados anonimizados. Esse é um conceito muito importante da Lei Geral de Proteção de Dados. Anonimizar os dados significa transformá-los de modo que seja possível não associá-los a uma pessoa. Seria como mascarar os dados a ponto de não conseguirem mais associá-los a uma

única pessoa, transformando os dados de alguma maneira. Esse é um processo que se espera que garanta a privacidade da pessoa.

Existem vários métodos de anonimização, e eles normalmente são aplicados quando é preciso divulgar os dados para pessoas que não têm o interesse primário naqueles dados de tratamento.

Por exemplo: se uma pessoa quer divulgar os dados de saúde pública e gostaria de inserir quais são os pacientes que tiveram no seu ambiente de saúde acamados e não seja possível citar o nome daquelas pessoas, então é possível colocar ali um outro identificador de modo a se mascarar aquele conjunto de dados. Isso é o que se chama de anonimização.

Existem vários processos para anonimização e o software que normalmente trata esses dados no ambiente do escritório de contabilidade já deve estar prevendo métodos de anonimização eficientes para prover essa proteção dos dados individuais. (BOFF et al, 2018).

Ressalta-se que a LGPD é muito abrangente, ela não fala só sobre os dados. Atualmente, a maioria dos dados são tratados no computador , mas é muito comum, por exemplo, que pessoas façam aleatoriamente uma impressão, use uma folha de rascunho que já foi impressa com dados das pessoas, utilize o verso da folha para fazer uma anotação ou uma agenda constando os dados de seus clientes. Diante disso, é muito importante proteger esses dados também. A lei não discrimina a mídia de dados, então em tese todos os dados estão cobertos pela lei. (BOFF et al, 2018).

A lei prevê diante do uso de dados pessoais que os dados de interesse legítimo da empresa não precisam ser os dados anonimizados, mas ao se recolher todos os dados pessoais é muito importante se ter um documento que esclareça à pessoa que ela está consentindo sobre o uso daqueles dados, é o que se chama de Termo de Consentimento Livre Esclarecido.

3.2 FIGURAS IMPORTANTES NO TRATO DA LGPD

Existe uma pessoa, uma figura que a lei geral de proteção de dados criou, que é o controlador dos dados. Ele vai ser qualquer pessoa física ou jurídica que coletar as informações, que coletar os dados da pessoa natural.

Nesse sentido, importa salientar que a LGPD é feita tão somente para quem coletar dados e informações de pessoa natural, de pessoa física. Já existem diversas

leis, como a lei do software, a lei do direito autoral, por exemplo, que regulamenta a coleta dessas informações, por isso o controlador de dados será a pessoa responsável por coletar essas informações (CANDELORO, RIZZO, 2012).

É possível exemplificar essa pessoa como um médico que ao coletar informações do seu paciente, na LGPD ele será chamado de controlador. Será ele quem irá captar os dados do titular, que é a pessoa natural e controla o seu armazenamento. Conforme preceitua Boni (2019), é ele que vai precisar dizer porque coleta esses dados, para qual finalidade, por quanto tempo ele irá armazenar esses dados, onde ele armazena e o que vai acontecer caso esses dados sejam expostos, ainda, será ele que vai precisar responder a essas perguntas e vai precisar criar todo um compliance para isso.

O controlador de dados é então a pessoa responsável por manter seguro todos esses dados e por ter a lealdade na sua coleta, inclusive, para dizer se vai compartilhar esses dados com alguma outra pessoa e por qual finalidade ele o fará.

Será o controlador de dados, portanto, uma das pessoas que vai sofrer maior impacto e a maior responsabilidade no que tange à lei, tendo em vista que no caso da não adequação caberá ao controlador ter que responder pelas multas pecuniárias das quais vão de 2% sobre o faturamento anual por cada infração até o limite de 50 milhões de reais, até mesmo a perda do direito de coletar essas informações (CANDELORO, RIZZO, 2012).

Assim, é possível imaginar um médico que perder o seu direito de coletar informações de seu paciente, ele terá praticamente inviabilizada a sua profissão, inviabilizada a sua carreira profissional.

Portanto, tem-se na figura do controlador de dados uma espécie de contador responsável pela coleta das informações do seu cliente, para declarar o imposto de renda, será o advogado que coleta as informações do seu cliente para manejar uma ação, para protocolar uma ação, poderá ser o porteiro que vai coletar a biometria da pessoa para poder autorizar a sua entrada num prédio, por exemplo (BONI, 2019).

Nesse sentido, é possível salientar que o controlador de dados será aquela pessoa que a lei encontrou para trazer essa informação, para capturar essa informação da pessoa física ou da pessoa natural como diz a lei. Por isso, se o empresário, por exemplo, coleta dados de qualquer natureza, seja de pessoa física ou de pessoa natural, ele é um controlador e vai precisar fazer a adequação à lei (BOFF et al, 2018).

Quanto ao papel do encarregado da proteção de dados, existe um ponto em que a lei certamente cria uma burocracia e certamente vai criar um custo a mais para os negócios foi uma figura nova na lei geral de proteção de dados, o chamado de ‘encarregado de proteção de dados’. A lei determinou que qualquer pessoa que precisar fazer adequação na LGPD, obrigatoriamente, precisará ter um encarregado de proteção de dados no seu quadro de pessoal. (BOFF et al, 2018).

O encarregado de proteção de dados é, então, a figura responsável por verificar as normas e procedimentos internos da empresa, para verificar se todos os funcionários estão adequados à lei geral de proteção de dados, se todos estão cumprindo as rotinas de forma adequada, em conformidade com a lei.

Caberá ao encarregado de proteção de dados a responsabilidade por receber, por exemplo, a fiscalização, por receber a autoridade nacional de proteção de dados, o Ministério Público ou mesmo para prestar contas, esclarecimentos aos clientes, ao titular dos dados que fizer as típicas perguntas como: Por que você armazena os dados? Onde esses dados são armazenados? Por quanto tempo? Qual a segurança que você dá para esses dados? Você compartilhará com alguém? (BOFF et al, 2018).

Será então o encarregado de proteção de dados a figura física, a personificação da utilização e do emprego correto dessas normas e da adequação à lei geral de proteção de dados.

A LGPD em seu art. 41 não estabelece quem não vai precisar da LGPD, o que significa que todas as empresas, de qualquer porte ou mesmo as pessoas físicas vão precisar nomear um encarregado de proteção de dados do qual vai precisar ter conhecimentos abrangentes tanto em TI ou tecnologia da informação quanto conhecimentos em direito para prestar esses esclarecimentos e informações e fazer as cobranças necessárias para a devida adequação da lei. (CANDELORO, RIZZO, 2012).

De tal modo, é possível perceber que a lei criou uma nova profissão, já que a quantidade de empresas que vão precisar desse tipo de profissional são inúmeras. Algumas empresas precisam contratar um carregador de proteção de dados externos para o seu quadro pessoal exercendo essa única finalidade, dependendo do volume de informações que são coletadas ou se tratando de empresas menores ou de profissionais liberais com uma menor quantidade de tratamento de informações. A recomendação é que seja nomeado alguém da própria equipe com essa nova atribuição e função.

Obviamente, que vai ter que ser apurada a responsabilidade tanto desse encarregado quanto da própria empresa para que não haja acúmulo de funções e uma possível ação trabalhista. Essa orientação, inclusive, os empresários precisam ficar cientes junto aos seus contadores e advogados de confiança (BONI, 2019).

Dando sequência à série dessas importantes figuras da lei geral de proteção de dados é importante mencionar uma importante figura chamada 'operador' de dados, que é a pessoa que irá operacionalizar todas essas informações coletadas pelo controlador. O operador poderá, ainda que isso seja muito difícil de acontecer na prática, a mesma pessoa que o controlador porque o operador será o responsável por tratar todos os dados.

Será o operador a pessoa que geralmente vai ser contratada para poder fazer o armazenamento dessas informações, o *compliance*, a guarda, toda a estratégia de proteção das informações. Nesse sentido, importa salientar que:

> O compliance se caracteriza como um conjunto de regras, padrões, procedimentos éticos e legais, que, uma vez definido e implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como a atitude dos seus funcionários (CANDELORO, RIZZO, 2012. p. 154).

É possível exemplificar essa pessoa através da figura do médico que coleta as informações do paciente no prontuário físico. Ele geralmente será o controlador e o operador, pois ele irá coletar as informações e irá armazená-las por meio dos usuários físicos dentro das suas gavetas, dentro do seu arquivo. Caberá a ele dizer quem terá acesso às informações ou não, ele quem vai criar todas as políticas para controlar essas informações. Então será ele tanto o controlador quanto o operador, a pessoa que vai tratar esses dados (CANDELORO, RIZZO, 2012).

Mas ele pode ser a pessoa que tiver um prontuário eletrônico, por exemplo, um advogado que trabalha com armazenamento de informações em nuvem, o operador será, por exemplo, o dropbox. O operador será aquele responsável pelo sistema daquele prontuário eletrônico, ou ainda será qualquer outra empresa contratada para armazenar essas informações digitais, para armazenar essas informações em nuvem, por exemplo.

Então, o titular será a pessoa natural que oferecerá as informações; o controlador será a pessoa que coleta as informações e o operador será aquele que vai tratar todos esses dados (BONI, 2019).

A lei geral de proteção de dados deu uma quantidade infindável de sinônimos para o tratamento de dados. O tratamento é a coleta, a guarda, a modificação, a alteração. Existem diversos sinônimos técnicos para que não haja discussões sobre quem pode ser o operador desses dados (BONI, 2019).

Em razão do seu dever de guarda, de informação e de proteção desses dados, o operador poderá ser solidariamente responsável com o controlador, caso eles não sejam a mesma pessoa.

Ou seja, no caso do vazamento de dados, de informações, por exemplo, ou de uma política inadequada no que tange ao tratamento de dados ou do armazenamento desses dados, o controlador será a pessoa acionada pelo titular ou pela fiscalização e o controlador poderá fazer aquilo chamado pela lei de ‘chamamento ao processo’, portanto, de trazer o operador para a ação, para responder igualitariamente com ele, caso exista alguma condenação.

> Por exemplo, um incidente de vazamento de dados em que, no decorrer do procedimento, seja apurado que também havia um tratamento de dados pessoais excessivo ou desproporcional. Poderá haver uma infração pelo incidente e outra pela ilicitude do tratamento. Ainda, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea (MACIEL, 2019, p. 271).

Nesse sentido, é possível perceber a importância e responsabilidade que o operador desses dados terá junto ao controlador no tratamento dessas informações, desses dados. Incumbe ao operador, portanto, essa responsabilidade, será ele que vai pagar juntamente com o controlador, caso alguma penalidade seja imposta, tanto sobre a proibição do direito de coletar dados, ou seja, de operacionalizar esses dados, quanto pelo pagamento dessas multas pecuniárias, dessas multas de dinheiro que a lei estabelece.

4 SEGURANÇA DE DADOS: IMPORTÂNCIA PARA AS ORGANIZAÇÕES

Acerca do impacto da Lei Geral de Proteção de Dados – LGPD no dia a dia das empresas, a lei traz hipóteses em que é possível coletar os dados do cliente de forma lícita. Quase todas elas se aplicam à realidade das empresas, sejam elas públicas ou privadas, mas não vai existir necessariamente uma hipótese específica.

Quando isso acontecer sempre vai existir a via do consentimento que certamente é a mais difundida entre as hipóteses de coleta de dados, no entanto é a mais frágil, é a mais complicada de usar porque ela pode ser revogada a qualquer tempo, ou seja, o cliente pode fornecer livremente um dado e depois ele mudar de ideia e pedir que a empresa elimine esse dado da sua base.

> O advento da LGPD se deve muito em razão do amadurecimento nas últimas décadas sobre a importância da informação. Quanto mais transparência e conscientização houver em torno do tratamento de dados, menos abusiva e desonesta será a conduta das empresas, e mais confiável, palpável e eficaz será a privacidade dos usuários (SEBRAE, 2021, p. 23).

Além do mais, o consentimento tem que ser dado de forma específica, clara e explícita. O empresário ao coletar o consentimento do seu cliente deve fazer isso dessa maneira, criando um campo específico para aquele consinta com o fornecimento daquele dado, de modo que não haja consentimento implícito, mas sim claro, explícito, dado livremente.

> Os dados pessoais dos consumidores sempre foram atraentes para o mercado. Com dados precisos sobre os consumidores é possível, por exemplo, organizar um planejamento de produtos e vendas mais eficiente, ou mesmo uma publicidade voltada às reais características dos consumidores, entre diversas outras possibilidades. Há pouco tempo atrás, o custo para se obter tais dados pessoais costumava restringir severamente a quantidade destas informações que eram efetivamente coletadas e utilizadas (BRASIL, 2010, p. 09).

Salienta-se que outra via de coleta e tratamento de dados pessoais é o legítimo interesse. Como o próprio nome diz, é o interesse que a empresa tem em coletar o dado, seja para a promoção das suas atividades, seja para proteger o cliente.

Um exemplo da promoção de atividade da empresa em que pode haver o legítimo interesse na concessão dos dados para a coleta, é quando uma empresa oferece um cupom promocional de aniversário, mas para isso ela precisa colher a

data de nascimento daquele cliente. Então, o cliente decide fornecer ou não, mas ela tem um legítimo interesse, ela quer promover as atividades dela oferecendo um benefício. Não tem nada de ilegal nisso.

> A LGPD estabelece proteções específicas aos dados pessoais de crianças e de adolescentes. Essa inovação foi pensada para evitar o uso inapropriado de informações relacionadas a menores de idade, o que pode colocar sua integridade em risco. De acordo com o Estatuto da Criança e do Adolescente, considera-se “criança” a pessoa até 12 anos de idade incompletos e “adolescente” aquela entre 12 e 18 anos (SEBRAE, 2021, p. 15).

Por outro lado, o legítimo interesse pode consistir na proteção ao próprio cliente, e se reverter em proteção para a própria empresa. É o que acontece com as políticas de prevenção de fraude. Muitas vezes, elas têm a necessidade de ter uma base robusta de dados para que não aconteçam fraudes que possam gerar prejuízo para o cliente e, consequentemente, prejuízo da própria instituição bancária.

Objetivamente, existem alguns principais tipos de impactos da LGPD na rotina das empresas. O primeiro deles é o impacto na relação e na comunicação com o cliente, ou seja, é como a empresa vai fazer e como ela irá montar sua estratégia de negócios, de modo a conseguir um dado que precise sem perder esse cliente de vista.

Para isso, é preciso que ela construa sua política de proteção e segurança de dados de forma clara e precisa, com linguagem acessível para que o cliente possa compreender e confiar no que a empresa está dizendo.

> A utilização de sistemas informatizados em diversas etapas da cadeia de produção e de consumo, à qual hoje já estamos nos habituando, trouxe consigo uma possibilidade concreta de mudança nesta equação: os sistemas informatizados de hoje têm uma capacidade muito grande de armazenar cada detalhe e sutileza das ações que ajudam a realizar. O consumidor de hoje existe em um ambiente onde muitas de suas ações são, ao menos tecnicamente, passíveis de registro e de posterior utilização (BRASIL, 2010, p. 09).

O segundo impacto é o impacto direto na coleta e na análise desses dados pessoais. Talvez a empresa precise despender um pouco de recursos para tornar a proteção desses dados efetiva e para tornar a sua base de dados segura, de modo que não haja violação, tendo em vista que a violação gera sanção e pode gerar um prejuízo para a empresa. Então, provavelmente é mais vantajoso para a empresa investir em proteção de dados do que arriscar uma eventual penalidade.

> Se por um lado cresce a cada dia o número de empresas que disputam os consumidores da internet [...] com preenchimento de formulários e cadastros, por outro lado cresce também o nível de conscientização dos consumidores quanto à possibilidade de aplicação do atual código do consumidor, que trata da matéria de utilização de informações de consumidores para fins comerciais, trazendo uma série de penalidades para quem a pratica (PECK, 2002, p. 37).

O terceiro grande impacto refere-se à rotina dos colaboradores da empresa. É sabido que para os microempresários e microempreendedores pode ser muito difícil ter um corpo funcional completamente capacitado ou designar um empregado para ficar exclusivamente responsável por esse assunto, mas é importante disseminar os princípios básicos da lei e manter aquele corpo de colaboradores atualizados sobre o que a lei diz para que o cliente se sinta seguro em fornecer os dados e para que aquela empresa tenha uma base de dados segura.

Outro impacto possível de ser citado, é o impacto nos custos, e ele dialoga com todos os outros listados. É possível ter custo com adequação das políticas da empresa na LGPD ou é possível ter custo com multas e penalidades. De tal modo, conforme preceituam Pimenta e Quaresma (2016, p. 535):

> A informação representa o recurso mais precioso para a organização, pelo que garantir a sua segurança é um dos maiores desafios com que as organizações têm que lidar. Frequentemente são aplicadas grandes quantidades de dinheiro e tempo em soluções técnicas, não considerando o fator humano (...) os usuários nas organizações têm um papel crucial na prevenção e detecção das violações de segurança. Para que exista uma segurança realmente eficaz, os usuários têm que agir de uma forma consciente, cumprir as políticas de segurança da organização e adotar comportamentos que não comprometam a segurança dos SI.

As multas que a LGPD prevê são muito altas. Elas chegam a 50 milhões ou a 2% do faturamento da empresa, o que for maior. Por isso é possível dizer que é melhor investir em prevenção, ou seja, é melhor investir para proteger os dados do cliente, para que se possa ter uma base de dados segura , do que arriscar sofrer uma penalidade.

4.1 NORMAS PARA ADEQUAÇÃO DAS EMPRESAS À LGPD

É muito comum o empresário ou empresária, de todos os ramos e portes estarem se perguntando se a LGPD é para aquela empresa. E a resposta muito direta

para este tipo de questionamento é sim. A LGPD é para todas as empresas que têm atividade econômica no Brasil, de qualquer segmento ou de qualquer porte, seja um pequeno empresário, seja uma empresa de pequeno porte, de grande porte, empresas de capital aberto, etc. Conforme o SEBRAE (2021, p. 04):

> A LGPD engloba todos aqueles que realizarem um tratamento de dados, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que os tratamentos sejam realizados em território nacional. Abrange também todas as empresas estabelecidas em território nacional, bem como as organizações com sede no exterior que ofereçam produtos/serviços para pessoas localizadas no Brasil ou tenham operações no País envolvendo tratamento de dados.

Portanto, todas as empresas, de qualquer segmento, seja para quem trabalha com e-commerce, quem não tem nenhum ambiente digital no seu negócio, para empresas que trabalham com Indústrias, para empresas de clínicas médicas, escolas, escritórios jurídicos, ou seja, todo mundo está atingido pela LGPD e precisa se adequar a ela.

> Diante disso, nasce a necessidade de compreender quais serão as alternativas para a adaptação das organizações quanto ao uso, divulgação, e armazenamento de dados e informações. Com a sanção presidencial, em agosto de 2018, as empresas terão até fevereiro de 2020 para se adequarem às novas regras. As empresas que demonstrarem conformidade e responsabilidade em relação às novas regras poderão alavancar uma vantagem competitiva no uso correto desses dados, aumentando o nível de confiança do seu público (SEBRAE, 2021, p. 04).

Outro esclarecimento muito importante é que essa lei já está valendo, sendo que ela entrou em vigor no dia 18 de setembro de 2020, portanto, já está valendo em todo o território nacional. E para se adequar à LGPD existe uma série de providências que precisam ser adotadas, tanto para microempresário, quanto para empresário.

> A LGPD tem como princípio fundamental a proteção de dados pessoais e o objetivo central de garantir ao titular mais autonomia em relação ao uso dos seus dados. A nova cultura imposta pela lei provoca um grande impacto na atividade empresarial, exigindo adequações operacionais no tratamento de dados, para que a privacidade e a transparência andem lado-a- lado (SEBRAE, 2021, p. 23).

A primeira delas, que é super importante, é que cada empresa precisa indicar, nomear uma pessoa do seu quadro funcional para ser o encarregado de proteção de dados pessoais. Trata-se de novo cargo criado pela LGPD e que atualmente, da

forma como a lei foi inserida no país, todas as empresas estão obrigadas a ter esta função.

Todavia, acredita-se que quando houver novos regulamentos, que estes passem a se tornar mais específicos, alguns pequenos negócios talvez possam ficar desobrigados de ter essa função, que é o encarregado de proteção de dados.

Nesse sentido, o que essa pessoa deve fazer é assumir a função de ser o contato entre os titulares de dados e a empresa, e o canal de comunicação também entre a empresa e a autoridade nacional de proteção de dados, portanto, uma espécie de agência reguladora que foi criada pela LGPD.

Outra providências a ser tomada pelas empresas, é ter uma base de dados bem volumosa com dados de clientes, dados de todas as pessoas físicas. É muito importante que o empresário desenhe um fluxo para atender aos requerimentos dos direitos dos titulares.

Existem empresas de grande porte que na época da vigência da lei têm se preparado bastante, mas mesmo assim, quando tiveram que lidar com problemas a respeito da lei em suas empresas, precisaram parar o seu time por alguns dias seguidos para atender a todas as demandas que chegavam dos clientes.

Então, é importante ao micro empresário ou empresários em geral se atentarem se eles estão preparados para isso. É importante então que eles tenham diante de si um desenho desse fluxo a fim de saber como ele vai implementar essa lei, esta rotina no seu negócio.

Importa salientar que o SEBRAE aponta alguns benefícios para as empresas com a LGPD, sendo eles:

> Melhora no relacionamento entre empresa e consumidor: com a transparência entre o cliente e a marca ainda maior, a empresa passará mais credibilidade e confiança aos consumidores.Maior regulamentação: com a lei unificando as regras sobre privacidade de dados, todas as empresas estarão alinhadas e cientes das sanções em caso de descumprimento às regras. Melhora o marketing da empresa: com a LGPD, as empresas precisarão eliminar informações irrelevantes, como endereços de e-mail inexistentes ou leads perdidos; com isso, o banco de dados estará mais organizado e apenas com dados dos clientes mais qualificados e engajados com a marca, gerando assim mais leads e, consequentemente, mais vendas. A empresa se comunicará apenas com os clientes que querem realmente saber mais sobre a sua marca. Mais segurança: a lei incentiva as empresas a aprimorarem a segurança da web e a adotarem medidas administrativas e técnicas adequadas para proteger os dados pessoais dos cidadãos, para controlar e monitorar qualquer violação de dados. Melhora a organização e gerenciamento de dados: será necessário organizar os processos de gerenciamento de dados para estar em conformidade com a lei. Essa organização será benéfica para a administração geral da empresa (SEBRAE,

2021, p. 21).

Dentre as providências mínimas que é possível dizer que também são importantes, está a construção de uma política de privacidade e proteção de dados. Provavelmente o empresário vai precisar do auxílio de um advogado para construir esse documento.

Logo, esse documento tem por finalidade ser transparente, é necessário mostrar para os clientes e para todas as pessoas físicas que se relacionam com aquele negócio como é feita a coleta de dados, que tipo de dados são coletados, o uso que é feito com cada um desses dados, ou ainda com quem esses dados são compartilhados. Isso implica na maneira de se dizer para todas as pessoas que aquele empresário é uma empresa preocupada com a proteção da privacidade dos seus clientes.

Outra providência refere-se à necessidade de se fazer um inventário de dados, onde então o empresário vai precisar mapear todos os dados de pessoas físicas que estejam nos bancos de dados do seu negócio.

Todavia, conforme Santos e Júnior (2018), importa salientar que quando se falou em banco de dados, leia-se: caderninhos , informativos grudados na tela do computador, arquivo que não se olha mais, caixas com dados de pessoas, de clientes antigos inclusive; então não só nos sistemas, mas também aqueles dados que estão no ambiente físico. Obviamente isso implica num grande trabalho, mas é importante que isso também seja realizado.

Esse trabalho de coleta de inventário, coleta de dados, tem por finalidade atender a lei da LGPD a fim de identificar o enquadramento legal, portanto, a fim de responder aos seguintes questionamentos: Por que você tem esse dado ? Você está autorizado a armazenar esse dado, a transferir esses dados para um terceiro? Você tem alguma base legal que justifique manter este dado dentro da sua organização?

São dez bases legais que a LGPD autoriza que as empresas tratem dados de pessoas físicas, encontrando alguma delas, o empresário pode seguir com sua operação, com aquela atividade específica para a qual ele faz o uso de dados. Entretanto, se ele não conseguir se enquadrar em uma dessas 10 hipóteses previstas na LGPD, infelizmente ele estará praticando uma irregularidade, passível de punição diante da LGPD.

> Os agentes de tratamento (controlador e/ou operador) que violarem as normas previstas na LGPD estarão sujeitos à aplicação de advertências, multas, sanções administrativas pela Autoridade Nacional, que são:• Advertência, com indicação de prazo para adoção de medidas corretivas;• Multa simples de até 2% (dois por cento) do faturamento da empresa, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, e limitada no total de R$50.000.000,00 (cinquenta milhões de reais) por infração;• Multa diária, observado o limite previsto no item acima;• A publicização da infração;• Bloqueio dos dados pessoais aos quais se refere a infração até a sua regularização;• Eliminação dos dados pessoais aos quais se refere a infração (SEBRAE, 2021, p. 22).

Outra providência para se adequar à LGPD é criar ou reforçar uma política de segurança da informação, se aquele negócio ainda não tem uma regra expressa, forte em proteger dados, então é o momento de se construir uma.

Conforme Santos e Júnior (2018) se o empresário já possuir uma ótima regra de proteção de dados, talvez seja o momento de atualizá-la para além de proteger a informação do seu negócio, aquela na qual o empresário possa já se preocupar há alguns anos, mas também no sentido de proteger os dados dos clientes existentes no seu banco de dados, e para isso existem medidas tanto tecnológicas quanto organizacionais.

Assim, é importante também se fazer uma hierarquia de acesso, tendo em vista normatizar quais empregados e colaboradores podem ter acesso ou não a determinado banco de dados. É o momento de colocar em prática uma política de atualização das senhas de e-mail a cada 3 meses, tudo aquilo que é muito corriqueiro se saber, mas que é comum sempre deixar para depois. Tudo isso com vistas à adoção de medidas para proteger esses dados pessoais.

Algo importante em relação à LGPD é guardar evidências de que aquele empresário era uma empresa madura em relação ao processo de proteção de dados, pois se ele tiver algum problema no futuro de vazamento de dados é possível que ele possa diminuir essa penalidade, a sanção da multa que ele pode levar, ou até mesmo anular essa multa. Isso pode ocorrer caso o empresário comprove que adotou todas as medidas possíveis de segurança de proteção de dados.

E dentre as medidas mínimas, as providências mínimas para que seja possível adequar o negócio à LGPD, é possível dizer que fazer o treinamento dos empregados e colaboradores é imprescindível.

O empresário pode até estar disposto a investir em recursos tecnológicos para proteger o seu banco de dados, proteger as informações, mas a ação humana é uma das grandes vulnerabilidades que se pode ter. Então, um empregado que sai

daquele corpo funcional, que é desligado pode levar dados daquele empresa, ou ainda, alguém pode fazer algo muito mais simples, como tirar uma *selfie* dentro do ambiente de trabalho e naquela imagem capturar dados que não deveriam, isso é um vazamento de dados e o empresário pode ser sancionado por isso, receber uma multa por ações deste tipo. Então, treinar as pessoas é super importante (SANTOS; JÚNIOR, 2018).

Tudo isso são, portanto, algumas dicas de providências mínimas dentro de um processo de adequação à LGPD. É óbvio que existem outros passos, mas o principal é se ter em mente que não existe uma fórmula para esses tratamentos de dados, é importante se ter cuidado com essas "fórmulas rápidas de implantação de LGPD com apenas um clique", muito corriqueiras de aparecer na mídia em geral.

As ferramentas tecnológicas podem auxiliar sobremaneira, em alguns casos elas são indispensáveis, elas até contribuem com a adequação à LGPD, no entanto, em alguns casos pode ser preciso um grupo multidisciplinar para atuar na adequação completa daquele negócio, dentro desse grupo vão estar profissionais da advocacia, profissionais especializados em processos e rotinas, profissionais de tecnologia da informação.

Por isso, manter-se informado é imprescindível, talvez com a própria equipe interna, o empresário consiga desenvolver um trabalho desse tipo, se não cabe a ele contar com a ajuda de profissionais terceirizados.

4.2. COMERCIALIZAÇÃO DE DADOS DE CLIENTES

Basta um clique ou um cadastro equivocado e os dados pessoais de uma pessoa acabam sendo coletados e guardados numa espécie de banco de dados. Ainda que ela não imagine, em qualquer momento empresas, instituições e até pessoas físicas podem ter em suas mãos várias informações sigilosas de seus clientes. E quando menos esperam, o seu nome pode estar envolvido em fraudes e dívidas.

> Nos dias atuais, a economia globalizada e o acesso à informação informatizada permitem o armazenamento de dados de maneira cada vez mais fácil e rápida. Muitas entidades privadas possuem um extenso número de informações sobre seus consumidores e armazenam muitos dados, sem que exista um controle efetivo sobre os mesmos. Os cidadãos, frequentemente, são surpreendidos com o recebimento de correspondências,

> e-mails, telefonemas, nos mais variados dias e horários, sem ter o conhecimento de como os seus dados foram obtidos pelos fornecedores de produtos ou serviços. (SANTOS, 2008, p. 236).

Isso acontece porque o mercado bilionário tem trabalhado na comercialização de dados pessoais. Esses dados podem ser vazados através de um desenvolvedor que se utiliza de um aplicativo de teste de personalidade para acessar dados.

Geralmente, a obtenção de dados pessoais é feita na própria internet, por meio de robôs que acabam acessando sites que disponibilizam informações, e com isso eles conseguem capturar essas informações das pessoas.

> A monetização dos dados pessoais foi uma tendência amplamente antecipada e que hoje é vital para uma parcela bastante representativa de novos serviços e produtos. Em uma declaração que se tornou bastante popular, a Comissária europeia do consumo, Meglena Kuneva, deixou claro que “os dados pessoais são o novo óleo da Internet e a nova moeda do mundo digital”, tornando claro o advento de um novo terreno adentrado pelas relações de consumo, no qual o consumidor passava a ser, em si, a fonte de um ativo que são as suas informações pessoais, suscitando a necessidade de adequação das normas que regulam o consumo para que levem em conta esta nova situação (BRASIL, 2010, p. 10).

Muitas vezes até com a conjugação desses dados, de posse do nome, RG, CPF, nome da mãe, conseguem entrar em áreas mais restritas de alguns sites, e a partir daí coletar as informações. De tal modo, a pessoa que tem os dados pessoais coletados sofre inúmeros riscos. O principal risco que é possível mapear, é de fato se tornar vítimas de golpes, porque com base em informações pessoais, os golpistas podem utilizar da chamada ‘engenharia social’, e é muito mais fácil que a vítima caia num golpe, se alguém já se apresenta usando seus dados.

> A sociedade globalizada e informatizada dos dias atuais tornou facilitada a forma de captação e armazenamento de dados pessoais. Estes dados, portanto, traduzem aspectos da personalidade e revelam perfis de consumo, possuem valor econômico e importância para a publicidade e para o comércio. Por essa razão, é cada vez mais comum a comercialização de informações constantes em bancos ou cadastros de consumidores (SANTOS, 2008, p. 243).

Além disso, podem acontecer situações de serem criados documentos falsos, com uso dessas informações, serem criadas contas bancárias, ainda mais num universo de contas digitais, onde muitas vezes não é preciso ter o contato físico ali com a instituição, embora esta tenha o dever de checar essas informações. No entanto, se há ali o acesso a esses dados, é mais fácil que o golpista passe por outra

pessoa, seja para fazer qualquer tipo de cadastro em sites de compras, para a criação de contas bancárias, etc.

Todavia, no que tange à venda de dados, é mais difícil a comercialização de dados de clientes com a entrada em vigor da lei, mas não é impossível. O importante é a empresa verificar o consentimento, colher esse consentimento de forma clara, de forma precisa e de forma específica para que o cliente saiba que, além de coletar, tratar os dados, essa empresa pode eventualmente vendê-los. Conforme Santos (2008, p. 243):

> Ocorre que, se de um lado existe a necessidade de se proteger o direito fundamental à privacidade desses consumidores, de outro, deve-se preservar a garantia de livre acesso às informações da entidade privada que pretende repassar os dados, direito fundamental que, como já visto, inclui a liberdade de receber e transmitir informações por quaisquer meios, sem interferências.

Conforme o SEBRAE (2021, p. 04): “entre as ações proibidas pela LGPD estão a coleta, o uso e o armazenamento de dados de qualquer pessoa sem o consentimento, bem como a utilização dessas informações para práticas ilícitas ou abusivas”. E caso essa empresa deseje comprar dados de outra, é importante que ela conheça a política de proteção de dados e privacidade dessa empresa que quer vender os dados para prevenir que a primeira seja responsabilizada com a segunda numa eventual violação de base de dados.

Vale lembrar que o objetivo da LGPD não é acabar com nenhum tipo de mercado, mas apenas coibir práticas abusivas. Então se aquele negócio depende do compartilhamento de dados, é importante ir se ajustando, adequando à política de proteção de dados, é o que a LGPD exige. É importante ir colhendo o consentimento do cliente, afinal, nenhum cliente gostaria de ter os seus dados invadidos.

4.3. DIFICULDADE DE IMPLEMENTAÇÃO DA LGPD NAS EMPRESAS

Desde agosto de 2018, quando foi sancionada a Lei Geral de Proteção de Dados, as empresas começaram a discutir internamente como se adaptar a essa lei.

A primeira pergunta que surgiu para elas foi: por onde se deve começar? Essa pergunta é bastante delicada, as empresas discutem por ser uma lei quem deveria conduzir seria o jurídico, é ele que precisa definir o que a empresa tem que fazer; outras empresas discutem que por se tratar de dados quem deve conduzir e definir o

que tem que ser feito é a área de tecnologia e informação – TI. Conforme Oliveira et al (2019, p. 175):

> A preocupação com o tratamento de dados pessoais como desdobramento da privacidade é um efeito colateral da mudança de paradigma trazida pela “Quarta Revolução Industrial”, cujo tom é dado pelo fenômeno da "informacionalização da sociedade”, iniciado na década de 1970. Seus reflexos impactam diretamente tanto a atividade econômico-empresarial, quanto a atuação do próprio Estado, que, além de criar e consumir informação, controla o fluxo de informações.

Como visto as mudanças são muito grandes e o prazo foi muito curto. A LGPD afeta as mais diversas áreas das companhias, desde um RH, uma área financeira, uma área de marketing, área jurídica, e assim envolvendo profissionais dos mais diversos perfis.

Isso implica serem necessárias grandes mudanças nas tecnologias utilizadas, integrações entre elas, nos processos, em aculturamento e treinamento dos usuários. Tudo isso deveria estar pronto até o ano de 2020, todavia, é sabido que isso não é fácil, principalmente em grandes empresas.

Algumas empresas estrangeiras contam com o benefício de já terem feito a adequação para o GDPR europeu, e assim, podiam trazer tudo aquilo praticado lá para ser aplicado aqui no Brasil com algumas adequações. Entretanto, essa não é a realidade das empresas nacionais, que precisam aprender e entender processos, entender as colocações da lei, e ainda se adequarem ao que pode surgir de alterações na lei, ao longo do tempo. Oliveira et al (2019, p. 185) complementa:

> Este fenômeno se deve muito em razão do amadurecimento nas últimas décadas da importância da informação como ativo dotado de valor financeiro e de mercado, considerados, sobretudo, os aspectos da ‘maleabilidade’ e ‘utilidade’ da informação, que experienciam sua influência sobre as tomadas de decisão e a vida cotidiana em geral.

Todavia, o que é possível concluir é que deve se começar com a adaptação e a junção de todos os líderes das diversas áreas da empresa. O envolvimento dos líderes e o comprometimento destes é extremamente importante. Além disso, todas as áreas devem estar envolvidas; áreas como RH, logística, marketing, o próprio jurídico e a TI devem estar totalmente comprometidas com esse projeto.

O que é possível se ver também são perguntas do tipo: mas quem deve então liderar o projeto? É a área de TI, o marketing, o presidente da empresa? É possível

se dizer que cada vez mais as empresas estão optando por um líder dentro da área de compliance, a fim de garantir que não somente as atividades de TI e as atividades das demais áreas estejam adaptadas à lei, como assim expõe Oliveira et al (2019, p. 177):

> Inicialmente, o empresário que usa, coleta e armazena dados de qualquer pessoa deve observar, além da boa-fé, os princípios trazidos pela Lei 13.709/2018, no art. 6º, para se manter em compliance 5. Tais princípios apresentam-se discriminados com sua aplicação prática, o que facilita a sua incorporação pelas políticas de proteção de dados

Mas principalmente a interação com a Agência Nacional de Proteção de Dados ou até mesmo o Ministério Público esteja garantido da maneira mais apropriada. Então, em resumo, o que é possível se destacar é que a lei está vigente, todos precisam se adequar à ela, deve-se começar principalmente com a liderança da empresa, ou seja, todos os líderes de todas as áreas envolvidas com o cliente final devem estar totalmente engajados em se adequar e a se adaptar à LGPD.

5 CONSIDERAÇÕES FINAIS

A proposta desta pesquisa foi tratar sobre a lei geral de proteção de dados que recentemente entrou em vigor no país. Para tanto, a pesquisa foi dividida em três capítulos centrais, sendo que o primeiro deles se propôs a refletir os conceitos de privacidade e proteção de dados, convergindo para as legislações de proteção de dados pessoais, a guarda e disponibilização.

Assim sendo foi possível observar que a Lei Geral de Proteção de Dados considera dado pessoal como toda a informação que torna a pessoa identificada ou identificável, portanto, toda informação que permite saber quem é aquela pessoa, e esse dado é relacionado somente à pessoa natural, ou seja, a pessoa física. São somente as pessoas humanas, ele é um atributo humano. No que tange à guarda e disponibilização,observou-se que o marco civil da internet estabelece que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações devem preservar a intimidade, vida privada e imagem das partes envolvidas.

O segundo capítulo se propôs a evidenciar os principais aspectos da lei geral de proteção de dados, a LGPD e a anonimização de dados, além das figuras importantes no trato da LGPD. Assim, foi possível observar que a LGPD tem a função de determinar como as empresas deverão fazer o tratamento de dados dos brasileiros, ou seja, basicamente estabelecer parâmetros de como esses dados devem ser coletados, armazenados, processados e destruídos.

Nesses preceitos, observou-se que a lei geral de proteção de dados deu uma quantidade infindável de sinônimos para o tratamento de dados, ao qual refere-se à coleta, à guarda,à modificação,à alteração.

Já o terceiro capítulo visou discutir acerca da importância da segurança de dados para as organização, focalizando nas normas para adequação das empresas à LGPD, além de reflexões sobre a comercialização de dados de clientes, sendo possível observar que a LGPD é para todas as empresas que têm atividade econômica no Brasil, de qualquer segmento ou de qualquer porte, seja um pequeno empresário, seja uma empresa de pequeno porte, de grande porte, empresas de capital aberto, etc.

Assim, evidenciou-se que algo importante em relação à LGPD se deve por ela guardar evidências de que aquele empresário era uma empresa madura em relação ao processo de proteção de dados, pois se ele tiver algum problema no futuro de

vazamento de dados é possível que ele possa diminuir essa penalidade, a sanção da multa que ele pode levar, ou até mesmo anular essa multa, isso pode ocorrer caso o empresário comprove que adotou todas as medidas possíveis de segurança de proteção de dados.

Assim, é possível considerar que os objetivos propostos com essa pesquisa foram alcançados, tendo em vista que a mesma objetivou fomentar reflexões acerca da política de segurança da informação e a lei geral de proteção de dados ou LGPD, tendo sido possível refletir que o objetivo da LGPD não é acabar com nenhum tipo de mercado, mas apenas coibir práticas abusivas. Então, se o negócio depende do compartilhamento de dados, é importante às empresas irem se ajustando, adequando à política de proteção de dados, conforme a lei exige, é importante ir colhendo o consentimento do cliente, afinal, nenhum cliente gostaria de ter os seus dados invadidos.

Por fim, é possível ainda explicar como sugestão para futuros trabalhos relacionados ao tema, a possibilidade de aprofundar na temática a partir da proposta de um estudo de campo, ao qual possibilitaria observar de forma mais próxima como se daria a implementação dessa legislação na prática, portanto, como as empresas atuam no seu dia a dia em prol da segurança de dados de seus clientes.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799:** tecnologia da informação: técnicas de segurança - Código de Prática Para a Gestão da Segurança da Informação.Rio de Janeiro, 2005. 120 p. Disponível em: http://xa.yimg.com/kq/groups/21758149/952693400/ name/ABNT+NBR+ISO+IEC+17799+-+27001- 2005. Acesso em: 12 abr. 2021.

ASSOCIAÇÃO BRASILEIRA DE ANUNCIANTES. **Manual ABA para adequação à LGPD:** Orientações e boas práticas de governança de dados para publicitários. Disponível em: http://www.aba.com.br/wp-content/uploads/2019/06/ebook-aba-compliance-lgpd.pdf. Acesso em: 10 mai. 2021.

BOFF, Salete O.; FORTES, Vinícius B.; FREITAS, Cinthia Obladen de A. **Proteção de dados e privacidade:** dos direitos às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. **Constituição Federal da República Federativa do Brasil de 1988.** Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 12 abr. 2021.

BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 12 abr 2021.

BRASIL. **Código Civil.** -1. ed. São Paulo: Revista dos Tribunais, 2002.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo:** para além da informação credíticia / Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010. Disponível em: https://www.defesadoconsumidor.gov.br/images/manuais/vol_2_protecao_de_dados_pessoais.pdf. Acesso: 22 mai. 2021.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014.** Marco civil da internet [recurso eletrônico]: Lei n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2015. (Série legislação; n. 164).

BRASIL. **Lei 12.414, de 09 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm. Acesso: 10 abr. 2021.

CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins de; PINHO, Vinícius. **Compliance 360º:** riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan Editora Universitária, 2012.

CASTRO, Luis Fernando Martins. Proteção de dados pessoais – internacional e brasileiro. **Direito e Tecnologias da Informação.** CEJ, Brasília, 2002,n. 19, p. 40-45, out/dez. 2002. Disponível em: https://egov.ufsc.br/portal/sites/default/files/infojur1.pdf. Acesso: 08 abr. 2021.

COMISSÃO EUROPEIA. **O que são dados pessoais?** Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt. 2020. Acesso em: 05 mai. 2021**.**

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Privacidade e Proteção de Dados Pessoais.** Brasília, 2017.

FILHO, Demócrito R. Reinaldo. **Privacidade na sociedade da informação.** Dissertação apresentada ao Programa de Pós-Graduação em Direito da Faculdade de Direito do Recife/Centro de Ciências Jurídicas da Universidade Federal de Pernambuco. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/4642/1/arquivo6028_1.pdf. Acesso: 12 abr. 2021.

JORGE, Higor Vinicius Nogueira; WENDT, Emerson. **Crimes Cibernéticos:** ameaças e procedimentos de investigação. 2. Ed. Rio de Janeiro: Brasport, 2013.

LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo:Saraiva, 2012.

MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais:** Atualizado com a Medida Provisória nº 869/18 . RM Digital Education. Edição do Kindle, 2019.

OLIVEIRA, Ana Paula de. et al. A Lei Geral de Proteção de Dados Brasileira na prática empresarial. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR.** Ano 4 - Número 1 - Maio de 2019. Disponível em: http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2019/05/revista-esa-cap-08.pdf. Acesso: 24 mai. 2021.

PECK, Patrícia. **Direito Digital.** São Paulo: Saraiva, 2002.

PEREIRA, Marcelo Cardoso. **Direito à Intimidade na Internet.** Curitiba: Juruá Editora, 2006.

PIMENTA, Alexandre Manuel Santareno. QUARESMA, Rui Filipe Cerqueira. A segurança dos sistemas de informação e o comportamento dos usuários. **Revista de Gestão da Tecnologia e Sistemas de Informação.** Vol. 13, No. 3, Set/Dez., 2016.

Disponível em: https://www.scielo.br/pdf/jistm/v13n3/1807-1775-jistm-13-03-0533.pdf. Acesso: 22 mai. 2021.

RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. A Proteção de Dados Pessoais na Internet no Brasil: Análise de decisões proferidas pelo Supremo Tribunal Federal. In: **Revista Cadernos do Programa de Pós-Graduação em Direito.** PPGDir./UFRGS. Disponível em: http://seer.ufrgs.br/ppgdir/article/view/61960/39936 Acesso em: 10 abr. 2021.

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SANTOS, Taylane Fanni Nunes dos. JÚNIOR, Eurípedes Brito Cunha. **Marco civil da internet:** responsabilização do provedor de aplicações e conflitos entre direitos fundamentais. ANAIS –21ª SEMOC, Salvador, 22 a 26 de outubro de 2018. Disponível em: http://ri.ucsal.br:8080/jspui/bitstream/prefix/1145/1/Marco%20civil%20da%20internet.pdf. Acesso: 11 abr. 2021.

SANTOS, Janaina de Carli dos. A comercialização de dados cadastrais do consumidor e a ponderação em face da colisão entre os direitos fundamentais à privacidade e ao livre acesso às informações: análise de um caso. **Revista do Ministério Público do RS**, Porto Alegre, nº 60, ago./2007/abr./2008. Disponível em: http://www.amprs.com.br/public/arquivos/revista_artigo/arquivo_1246468845.pdfAcesso: 21 mai. 2021.

SEBRAE. LGPD. **Lei Geral de Proteção de Dados.** E-book. 2021. Disponível em: https://www.sebrae.com.br/Sebrae/Portal%20Sebrae/UFs/PE/Anexos/LGPD-Connect-Sebrae.pdf. Acesso: 22 mai. 2021.

TOMIZAWA, Guilherme. **A invasão de privacidade através da internet**. Curitiba: J.M. livraria jurídica, 2008.