Cognitio Juris
ISSN 2236-3009

A LGPD E OS LIMITES E RESPONSABILIDADE DOS PROVEDORES DE SERVIÇOS VIRTUAIS NO TRATAMENTO DE DADOS PESSOAIS

THE LGPD AND THE LIMITS AND LIABILITY OF VIRTUAL SERVICE PROVIDERS IN THE PROCESSING OF PERSONAL DATA

Artigo submetido em 09 de fevereiro de 2023
Artigo aprovado em 17 de fevereiro de 2023
Artigo publicado em 01 de março de 2023

Cognitio Juris
Ano XIII – Número 45 – Março de 2023
ISSN 2236-3009

Autores:
Leonardo Arruda Vilela Garcia[i]
Ana Carolina Nunes Lopes Cançado Garcia[ii]

Resumo: A utilização dos recursos e serviços de Tecnologia da Informação (TIC) representam agilidade, facilidade e eficiência na execução das atividades diárias. Na utilização desses serviços, muitas informações são deixadas pelos usuários, gostos, hábitos, opiniões e outros que possam individualizar as tendências acabam sendo registrados. A LGPD visa proteger todos os titulares dos dados (usuários de serviços), sendo estes digitais ou não, para que tenham seus direitos de privacidade assegurados. A proteção de dados pessoais é um direito fundamental e o respeito à privacidade e aos dados pessoais evitam a influência na determinação informativa, permitem a liberdades de desenvolvimento da própria

personalidade, a não influências na liberdade de pensamento e tomada de decisão não viciada pela influência de terceiros. Neste artigo analisamos e delimitamos e responsabilidades dos provedores de serviços virtuais no tratamento de dados pessoais, observada a necessária adoção das medidas técnicas, boas práticas e medidas administrativas para minimizar e evitar falhas de segurança na implementação da LGPD para a proteção usuários; evidenciamos as preocupações a nível mundial com o tema, finalizando com as considerações finais. Não houve a pretensão de esgotar todo o tema, em razão da sua complexidade e abrangência.

Palavras-chaves: LGPD. Agentes de Tratamento de Dados. Medidas técnicas para a proteção de dados. Direitos dos Usuários. Sanções administrativas LGPD. ANPD.

Abstract: Information Technology (ICT) resources and services represent agility, ease, and efficiency in daily activities. However, when using these services, such information is left by users, likes, habits, news, and others that individualize personal trends are registered. The LGPD aims to protect all data subjects (service users), whether digital or not, so their privacy rights are guaranteed. The protection of personal data is a fundamental right. Respect for personal data avoids the influence of informational determination, allows the freedom to develop one's personality, and does not influence liberty of thought and decision-making. In this article, we analyze and delimit the responsibilities of virtual service providers in the processing of personal data, observing the necessary adoption of technical, good practices, and administrative measures to minimize and prevent the occurrence of security incidents in the implementation of the LGPD to protect the rights of holders; we highlight the worldwide concerns with the theme, ending with the final considerations. However, due to its complexity and scope, there is no intention of exhausting the theme.

Keywords: LGPD. Data Processing Agents. Measures, techniques for data protection. User Rights. LGPD administrative sanctions. ANPD.

Sumário: Introdução. 1. Breve histórico da evolução das leis de proteção de dados 2. A LGPD e os agentes responsáveis pelo tratamento de dados. 2.1. Responsabilidade dos agentes de tratamento e a figurado encarregado de dados. 3. Medidas técnicas necessárias para proteção dos dados e dos direitos dos usuários. 3.1. Direitos dos usuários (titular dos dados pessoais). 4. A LGPD e a aplicação das medidas técnicas e administrativas ligadas a TIC. 5. LGPD, suas sanções administrativas e a Legislação penal. 6. A necessidade de proteção e a visão mundial sobre os dados pessoais. 7. Considerações Finais. Referências Bibliográficas.

Introdução

Sem dúvida a Tecnologia da Informação (TI), provida principalmente pelas soluções de Tecnologia da Informação e Comunicação (TIC), proporcionaram grande revolução nas relações humanas, principalmente na comunicação e nos negócios. As TIC representam fluidez nas comunicações, a rápida recuperação de informações e diversas vantagens na concretização e viabilização de negócios, permitindo agilidade e eficiência. Não restam dúvidas a respeito dos benefícios proporcionados.

O setor de tecnologia da informação cresceu em muitas direções, reduzindo a burocracia, reduzindo a fraude, aumentando a transparência, fortalecendo a auditoria e até reduzindo a corrupção. Todos esses benefícios se relacionam diretamente aos problemas crônicos da administração pública, e se estendem às organizações privadas, que seriam difíceis de obter sem o uso da tecnologia da informação (WEILL, ROSS, 2006). Os avanços tecnológicos proporcionaram uma revolução na comunicação, consequência disso é a avalanche de publicações e compartilhamentos de conteúdo. Para se ter uma ideia do grande volume de dados que são compartilhados e deixados nos meios digitais, as estimativas mais recentes do tamanho da população mundial, de acordo com a Organização das Nações Unidas (ONU)[iii] é de aproximadamente 8 bilhões de pessoas. Destas, de acordo com estimativas DATAREPORTAL[iv] 64,4% (5,16 bilhões), estão conectadas a internet, e 59,4% (4,76 bilhões) são usuários ativos de mídias sociais. O tempo médio mundial gasto no uso da internet é de

6,37 horas por dia navegando e deixando uma grande quantidade de dados (a média de uso do brasileiro é de 9,32 horas), o que pode ser perigoso para a privacidade e segurança implicando em exposição indevida de informações pessoais.

Nesse contexto, todo usuário (titular de dados) que de alguma forma utiliza provedores de serviços virtuais é passível de ter seus dados expostos, revelando suas atividades, informações acerca de si e outros dados sensíveis em razão do tratamento de dados desnecessário pelos provedores de serviços virtuais.

Um dado isolado, desconexo já carrega consigo potencial para lesar o seu titular, que o produziu, na medida em que seja traçada uma conexão entre vários dados suplementares e técnica específica, temos constituído um dado individualizável do seu titular (BIONI, 2019). É evidente que o abuso no consentimento para realização do tratamento de dados pode ocorrer, mesmo que esteja baseado no legítimo interesse. Na Lei Geral de Proteção de Dados (LGPD) há parâmetros suficientes para fundamentar que o tratamento de dados seja realizado nos limites da atuação empresarial, sendo que o caso em concreto determinará se há legítimo interesse no tratamento de dados (BRASIL**,** 2018).

A finalidade da LGPD é proteção dos direitos fundamentais básicos de liberdade e privacidade, para garantir o livre desenvolvimento da personalidade da pessoa natural, protegendo os dados pessoais e assegurando a propriedade desses dados. Desta forma, a coleta de dados que ultrapassa o necessário para atuação empresarial, além de configurar ilícito, configura verdadeira violação à privacidade e intimidade, excedendo os limites do tratamento de dados baseado no legítimo interesse. A proteção dos dados pessoais é um direito fundamental, assim, o consentimento no tratamento dos dados pelo titular não pode ser interpretado como uma doação, mas, a nítida e clara demonstração de confiança e boa-fé objetiva, gerando assim a obrigação do tratamento dos dados seja realizado com todo cuidado pelo fornecedor do serviço de TIC.

Este artigo pretende analisar, com base na LGPD, Guias e documentos expedidos da Autoridade Nacional de Proteção de Dados (ANPD), do Comitê Central de Governança de Dados (CCGD)[v] e outros aspectos técnicos da Tecnologia da Informação (TI) ligados a proteção de dados, delimitar quais são os limites e responsabilidades dos provedores de serviços virtuais de TIC no tratamento de dados pessoais, na implementação e aplicação das medidas técnicas e administrativas para evitar falhas de segurança da informação, os direitos dos titulares de dados, finalizando com as considerações finais. Não se pretende esgotar todo o tema, em razão da complexidade e abrangência. Realizaremos levantamento bibliográfico no que tange a LGPD e outros conceitos necessários para se delimitar quais as principais características necessárias aos provedores de serviços virtuais no tratamento de dados pessoais, as boas práticas na implementação da LGPD e as responsabilidades dessas entidades no tratamento de dados pessoais.

1. Breve histórico da evolução das leis de proteção de dados

As leis de proteção de dados surgiram como uma resposta ao crescente uso e armazenamento de dados pessoais pelas entidades e visam garantir que esses dados sejam tratados de forma justa e legal, protegendo os direitos dos indivíduos e garantindo que eles tenham controle sobre como seus dados são usados.

As Leis Gerais de proteção de dados, em um contexto global, são reflexo de um processo da evolução da tecnologia e da computação que permitiu e possibilitou o processamento e armazenamento de dados em escalas nunca antes imaginadas. Para Bioni a ciência computacional “revolucionou quantitativa e qualitativamente a capacidade de processamento” dos dados na obtenção de informações (BIONI, 2019, p. 156). Nesse contexto, MAYER-SCHONBERGER (1997) apresenta as quatro gerações de leis de proteção de dados na europa:

A primeira geração surge na década de 70, em que a coleta e processamento de dados dos

cidadãos impulsionaram o planejamento estatal, havendo temor da sociedade da desumanização da relação estado-cidadão. Assim, as leis de primeira geração estão ligadas aos controles dos bancos dados e ao condicionamento à prévia licença ou registro. O processamento e armazenamento dos dados são centralizados, marcados pelo uso de computadores de grande porte em que apenas grandes corporações tinham acesso. O foco da proteção concentra-se no processamento dos dados da sociedade, é uma tentativa de domar a tecnologia e os gigantescos bancos de dados. Ou seja, busca-se aqui uma liberdade negativa, um deixar de fazer do Estado e grandes entidades na direção de evitar intervenções arbitrárias.

Na segunda geração, a descentralização do processamento de dados é uma realidade, expondo a fragilidade das normas de primeira geração, que implica em nova atualização legislativa para permitir a proteção da privacidade como prioridade, sendo associada a proteção de dados, privacidade, liberdades individuais em geral e liberdades negativas, focando-se nos direitos individuais. Nessa geração, a principal característica é a possibilidade de participação do indivíduo na coleta e processamento de dados pelo consentimento e a ampliação dos poderes do Estado na prestação de dados pelas autoridades encarregadas de sua proteção, permitindo a delimitação dos espaços de intimidade do cidadão.

A terceira geração tem seu marco em 1983, com a decisão do Tribunal constitucional alemão sobre a inconstitucionalidade da “Lei do Censo”, em que o consentimento e a participação do cidadão no processamento de seus dados foi compreendido como necessário e contínuo em todo o processo. Outra característica é a impossibilidade de localização física dos bancos de dados que passaram a ser armazenados em rede. “O direito básico do indivíduo de determinar a liberação e o uso dos seus próprios dados pessoais” (p. 229).

A quarta geração promoveu a expansão das normas gerais sobre a proteção de dados e tentou resolver conflitos entre a violação da privacidade e o, incluindo o consentimento prévio ao tratamento dos dados, sendo constatado que dados pessoais sensíveis deveriam

ser retirados da esfera de disponibilidade em razão do elevado risco discriminatório. Um marco importante é a vigência da Diretiva 95/46/CE União Europeia em 1995 que trata da proteção dos dados pessoais e a sua livre circulação.

Em 2018, a UE adotou a Regulamentação Geral de Proteção de Dados (RGPD), que é uma lei mais abrangente e exigente que a Diretiva 95/46/CE. A RGPD aplica-se a todas as empresas e organizações que tratam dados pessoais de indivíduos na UE, independentemente de onde essas empresas estejam localizadas. Ela também estabeleceu o conceito de "controlador de dados" e "operador de dados", que são responsáveis por garantir o cumprimento da lei.

No contexto brasileiro, as legislações de proteção de dados, não eram estruturada em um único corpo normativo mas, sim, através várias normas, dentre os quais destacam-se: o Código de Defesa do Consumidor; a Lei de Acesso à Informação; o Marco Civil da Internet; os: decreto do Serviço de Atendimento ao Consumidor (Decreto n. 6.523/2008), decreto do Censo Anual da Educação (Decreto n. 6.425/2008) e decreto que regula o cadastro único para programas sociais do Governo Federal (Decreto n. 6.135/2007) (MENDES, 2014, p. 155-156). A LGPD unifica o sistema de proteção dos dados pessoais, e direciona o tratamento dos dados pessoais para ser realizado com base nas hipóteses legais de tratamento (OLIVEIRA, 2018, p.8-9).

Em resumo, as leis de proteção de dados têm evoluído ao longo dos anos, sendo aprimoradas para acompanhar o crescente uso e armazenamento de dados pessoais. Elas visam garantir que esses dados sejam tratados de forma justa e dentro dos parâmetros legais estabelecidos, protegendo os direitos dos indivíduos e garantindo que eles tenham controle sobre quais são os dados armazenados e principalmente de como são tratados.

2. A LGPD e os agentes responsáveis pelo tratamento de dados

A LGPD protege os direitos fundamentais básicos de liberdade e de privacidade, como garantias para assegurar o livre desenvolvimento da personalidade da pessoa natural,

dispondo dos parâmetros para o tratamento de dados pessoais. A lei define que o tratamento de dados abarca as atividades que utilizem de dados pessoais na execução de qualquer operação, aplicando-se a pessoas físicas (naturais) ou a pessoas jurídicas de direito público ou privado, abrangendo "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". Define também, que o tratamento, realizado por meio físico ou digital, deve ser realizado segundo os parâmetros definidos na LGPD, englobando um amplo conjunto de operações efetuadas por meios físicos (manuais) ou digitais (BRASIL**,** 2018). Além de regulamentar como será realizado o tratamento dos dados pessoais, a lei indica que seja feito de maneira transparente, segura, ética, para prevenir fraudes, o uso inadequado ou abusivo de informações pessoais, sendo fundamental garantir a segurança e evitar a ocorrência de danos aos dados.

A lei define que no tratamento dos dados o controlador e o operador são os responsáveis. Ambos se sujeitam às suas regras e à fiscalização da ANPD. Resumidamente, o controlador decide, de acordo com seus interesses e finalidades, como o tratamento de dados pessoais será realizado. O operador, executa o tratamento como definido pelo controlador, seguindo fielmente todas as suas definições, e em seu nome. Ambas são entidades distintas, não havendo grau de subordinação (ANPD, 2021b).

Pessoas físicas e jurídicas, seja de direito público ou privado poderão atuar como operadoras. Observamos que não existem impedimentos para que uma pessoa física seja contratada como operador. Para operador do tipo pessoa jurídica, temos um agente de tratamento formalmente definido pela LGPD, representada pelos seus funcionários. (ANPD, 2021b).

2.1. Responsabilidade dos agentes de tratamento e a figura do encarregado de dados

O controlador é o principal responsável por manter os registros das operações de tratamento, sendo que, caso o operador atue no tratamento, conforme determinado pelo art. 37 da LGPD, essa obrigação é compartilhada. Assim, nos termos do art. 42 da mesma lei, ambos, controlador e operador, possuem a obrigação de reparação se "causarem dano patrimonial, moral, individual ou coletivo a outrem", sendo necessária a reparação[vi].

O controlador e operador tem obrigações distintas, que em regra determinadas de acordo com o papel exercido na execução do tratamento de dados, mas, o operador responde solidariamente pelos danos causados por descumprimento das obrigações legais ou por deixar de seguir as instruções do controlador. Nesta hipótese, o operador se equipara ao controlador.

Seja controlador ou operador executando o tratamento dos dados pessoais, todos os agentes de tratamento devem adotar as medidas técnicas, administrativas e principalmente as medidas de segurança, de forma a proteger os dados pessoais, restringindo acessos não autorizados e de situações acidentais ou ilícitas que possam permitir o acesso, destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados pessoais sob a sua guarda e gestão. Devendo assim, impedir que haja qualquer incidente de segurança com dados pessoais, que podem ter as seguintes origens de acordo com o Centro de Estudos, Resposta e Tratamento de incidentes de Segurança no Brasil, dentre outras inúmeras situações aqui não elencadas, caso ocorram (CERT.br, [2021]):

a. do furto de dados por atacantes (terceiros) e códigos maliciosos que exploram vulnerabilidades em sistemas;
b. do acesso a contas de usuários, por meio de senhas fracas ou vazadas;
c. da ação de funcionários ou ex-funcionários que coletam dados dos sistemas da empresa e os repassam a terceiros;
d. do furto, descarte ou doação de equipamentos que contenham dados sigilosos;
e. de erros ou negligência de funcionários, como descartar mídias (discos e pen drives)

sem os devidos cuidados.

Em ocorrendo um incidente de segurança, citamos alguns exemplos de dados que eventualmente podem ser vazados (CERT.br, [2021]):

a. credenciais de acesso, como nomes de usuário e senhas;
b. informações financeiras, como números de contas bancárias e de cartões de crédito;
c. segredos industriais e comerciais;
d. informações pessoais e outros documentos, como CPF, RG e carteira de habilitação;
e. informações de contato, como endereços e números de telefone;
f. registros de saúde, como resultados de exames e prontuários médicos;
g. outros dados, como data de nascimento e nomes de familiares.

Para assegurar a conformidade de uma organização, pública ou privada, à LGPD, é necessária a indicação do encarregado de dados. O encarregado é o ponto de contato entre o controlador e a Autoridade Nacional de Proteção de Dados (ANPD) e titulares dos dados (usuários). A lei não especifica quais as circunstâncias de indicação de um encarregado e atualmente, não indica situações de dispensa, assim toda organização deverá indicar um encarregado. Conforme as boas práticas internacionais, o encarregado pode ser alguém que tenha vínculo direto com a instituição, um funcionário, ou um agente externo, de natureza física ou jurídica. A ANPD, recomenda que a indicação seja realizada por um ato formal, "contrato de prestação de serviços ou um ato administrativo" (ANPD, 2021b).

A ANPD, recomenda, e como boa prática, é importante que o encarregado tenha a autonomia, liberdade, e os recursos necessários para atuar, pontuando que são necessários os "conhecimentos de proteção de dados e segurança da informação em nível que atenda às necessidades da operação da organização". Mesmo com o encarregado indicado, é importante asseverar, que a responsabilidade pelo tratamento dos dados pessoais é do controlador ou do operador de dados. O encarregado atua para garantir a conformidade legal

e como ponto de contato com os usuários e a ANPD, sendo assim, seu contato deve ter o acesso facilitado (ANPD, 2021b).

Entende-se assim, com base em todo levantamento bibliográfico realizado, que o encarregado de dados, é o responsável por indicar e até mesmo auxiliar na implementação e implantação das políticas e práticas necessárias à proteção de dados dos titulares que são tratados. Assim, indica e executa as medidas técnicas de prevenção necessárias e adequadas para a proteção dados dentro das organizações para evitar, e minimizar, a ocorrência de falhas e outros incidentes de segurança com os dados pessoais.

3. Medidas técnicas necessárias para proteção dos dados e dos direitos dos usuários

Em se tratando de meio digital, a ocorrência de falhas de segurança é muita alta, e de difícil compreensão sem os conhecimentos técnicos necessários, desta forma, acessos não autorizados, seja este realizado acidental ou por meios ilícitos, que de alguma forma resultarem na manipulação e exposição de dados pessoais podem ocorrer. O vazamento de dados é um dos principais incidentes de segurança e pode implicar em prejuízos aos titulares dos dados. Com relação a este tema, o Tribunal de Justiça de São Paulo vem firmando entendimento, de que caso haja vazamento de dados pessoais por falhas no tratamento pelos agentes de tratamento, de não reconhecer o direito de reparação com base em potencial risco de utilização indevida de dados e prejuízo. Assim, não se admite o dano hipotético, sendo necessária a relação de causa entre o vazamento de dados a utilização indevida dos dados e os prejuízos causados ao titular dos dados.

São os principais riscos de dados vazados (CERT.br, [2021]): a) O Furto de identidade, que pode implicar na abertura de contas bancárias e a concessão de empréstimos, o uso de convênio médico por terceiros, o uso de documentos oficiais por terceiros que foram obtidos por meios fraudulentos, a realização de aquisições sem a necessidade de pagamento prévio,

o que implicará necessariamente em danos morais e prejuízos financeiros; b) Tentativas de golpe, como extorsão para que os dados não sejam expostos a público; c) Violação de privacidade, com a exposição de conversar particulares, dados médicos ou outras informações de interesse unicamente privado, além de outras situações aqui não citadas aqui.

Para evitar vazamentos de dados pessoais, a invasão e acesso não autorizado e a ocorrência de outros incidentes de segurança da informação, são necessárias à implementação e execução de medidas administrativa e técnicas de prevenção relacionadas a Tecnologia da Informação (TIC), que devem ser adequadas ou tratamento de dados e esteja em conformidade legal. Inclui assim, o planejamento e implementação de política de segurança da informação, políticas de anonimização e pseudonimização, criptografia, incluindo também, a não retenção desnecessária de dados pessoais, dentre outros. Abaixo detalhamos os aspectos e requisitos mínimos necessários quanto a estruturação de Segurança e Privacidade para os produtos de ou Serviços ligados a TIC (CCGD, 2021c):

a. **Política de Segurança da Informação (POSIN)** – Compreende o conjunto de diretrizes e regras que tem por objetivo planejar, implementar o controle de ações relacionadas à segurança da informação das organizações, sendo um instrumento para apoiar as organizações em estruturar todo o processo de segurança da informação que é adequado de acordo com o seu porte. A ANDP, incentiva a elaboração e a implementação da POSIN, pois independente do porte do agente de tratamento, evidencia a diligência e a boa-fé na segurança dos dados sob à sua tutela. Assim sendo, quando possível a POSIN, no caso de agentes de tratamento de pequeno porte, ainda que simplificada de ser estabelecida (ANPD, 2021a).
b. **Análise de Impacto na Privacidade de Dados Pessoais**: Há na LGPD previsão da elaboração de relatórios de impacto à proteção de dados. a proteção de dados pessoais é uma necessidade e preocupação mundial, como exemplo, a União Europeia possui o Regulamento Geral sobre a Proteção de Dados (GDPR), em vigor desde maio de 2018,

sendo inspiração para legislações no mundo todo. Na GDPR temos a previsão que a avaliação de impacto de proteção de dados pessoais, sempre que indicar que o tratamento dos dados possa implicar em elevados riscos para os direitos e liberdades individuais, deve ser realizada. Assim, devem ser indicadas as medidas que foram tomadas para que o tratamento esteja em conformidade legal. Quando o responsável pelo tratamento não puder atenuar os riscos com a implementação de medidas razoáveis com o uso da tecnologia disponível, a autoridade de controle deverá ser consultada antes do início das operações de tratamento (PARLAMENTO EUROPEU, 2016). A LGPD segue a mesma linha quando indica que a autoridade nacional poderá determinar ao controlador a elaboração do Relatório de Impacto à Proteção de Dados (RIPD). Nesse sentido, em se tratando de entidades privadas, o RIPD pode ser solicitado quando o tratamento de dados é realizado com fundamento no interesse legítimo, ou, a qualquer momento. Sendo um dos principais insumos para sua elaboração, é o inventário de dados pessoais, pois, trata-se de documento que descreve as informações sobre os tratamentos de dados pessoais realizados, verificando a conformidade legal da instituição na execução deste (CCGD, 2021c).

c. **Análise e Avaliação de Riscos**: Trata-se de análise e avaliação de riscos de arquitetura a solução de TIC, que deve ser realizada periodicamente e indica eventos de risco que o sistema possa estar exposto. Assim, orienta na identificação de lacunas de segurança da informação e de privacidade.
d. **Arquitetura, Controles de Segurança e Matriz de Responsabilidades:** Descreve a arquitetura física e lógica da solução de TIC, assim com os controles de segurança da informação e privacidade implementados nos componentes das arquiteturas. A Matriz de responsabilidades descreve as responsabilidades e os atores envolvidos na organização pela segurança da informação, privacidades, indica os gestores dos serviços com dados pessoais, assim como os operadores de tratamento relacionados.
e. **Continuidade Operacional e Contingência**: Manutenção da operação das atividades, busca-se garantir a continuidade das operações em situações de

indisponibilidade dos serviços de TI e outras situações adversas. Trata-se da necessidade de manter e implantar os Planos de Continuidade operacional e Plano de Contingência.

f. **Gestão de incidentes**:Registrar os incidentes de segurança da informação e privacidade ocorridos, coletando e preservando as evidências e outras medidas para reduzir a probabilidade e mitigação do incidente, incluindo comunicação aos titulares de dados e as autoridades competentes caso haja comprometimento dos dados.
g. **Coleta e preservação de evidências**: Necessidade de se implementar os controles necessários para a coleta e preservação de qualquer incidente relacionado a segurança da informação e privacidade.
h. **Gestão de Mudanças**: Controlar as mudanças de forma que não afetem a segurança da informação e privacidade dos dados pessoais;
i. **Desenvolvimento Seguro**: Os sistemas devem possuir e manter trilhas de qualidade e testes de software de forma que:
j. Os ambientes de testes passem por processo de anonimização;
k. A utilização de dados pessoais em ambientes de testes deve ser expressamente autorizada pelo controlador dos dados;
l. Adoção de técnicas ou métodos para exclusão ou destruição segura de dados pessoais, impedindo a sua recuperação;
m. Possuir funcionalidade para, ao se fornecer base de dados para órgão de pesquisa, que os dados sejam anonimizados ou pseudoanonimizados;
n. Aderência do sistema a LGPD para assegurar o tratamento adequado de dados pessoais, principalmente a classificação em sensíveis e não sensíveis;
o. Realização do RIPD na proteção de dados pessoais para a solução de TIC.
p. **Segurança das redes corporativas**: Assegurar a adequação do nível de segurança corporativa, incluindo Segurança Web, servidores de aplicação e banco de dados, para garantir o nível adequado de segurança da informação.
q. **Política de Backup**: Realizar os backups das informações e outros registros de logs,

de modo que seja possível a recuperação de versões dos sistemas, de base de dados e outras documentações associadas. Assim, em caso de desastres, existe a possibilidade de restauração dos serviços em tempo hábil.

Os requisitos mínimos necessários quanto a estruturação da segurança e privacidade para os produtos de ou serviços ligados TIC, tem caráter administrativo, sendo estruturais da organização para atuação em conformidade com LGPD. Abaixo descrevemos os requisitos de segurança da informação e privacidade, trata-se de requisitos técnicos ligados a TIC e ao fornecimento de serviços digitais. São os requisitos de segurança da informação e privacidade (CCGD, 2021b):

a. **Controles Criptográficos**: São necessários de acordo com o grau de sigilo necessário para as informações armazenadas, incluindo o tráfego pela rede e o tratamento dessas informações. Quanto maiores os tempos de guarda e retenção legal de uma informação, maior serão esses controles;
b. **Controle de Acesso**: Limitação do privilégio de acessos a sistemas e outras informações a somente ao necessário para execução de atividades específicas. O objetivo é reduzir o risco a qualquer incidente de segurança e limita-se a concessão de autorizações de acessos apenas ao necessário e suficiente, limitando os acessos a informações sensíveis;
c. **Registro de Eventos e Incidentes de Segurança**: Trata-se da necessidade de manter os registros e informações sobre os tratamentos realizados e outros eventos, incluindo falhas e incidentes de segurança da informação e privacidade;
d. **Registro de eventos e rastreabilidade**: Trata-se da necessidade de manter os registros sobre o tratamento dos dados realizados para que seja possível assegurar a rastreabilidade de ações de usuários pelos logs das transações executadas e acesso a sistemas. São importantes para a realização de auditoras e inspeções de conformidade com a LGPD;
e. **Salvaguarda de logs**: São necessárias a implementação de mecanismos para guarda

e proteção de dados relacionado aos logs armazenados, inclui outros registros de atividades dos operadores e administradores dos sistemas que não devem possuir perfil que permita a exclusão ou a desativação dos registros de log de suas próprias atividades.

f. **Compartilhamento, uso e proteção da informação**: São necessários a adequação dos controles para compartilhamento, uso e proteção dos dados quando houver a necessidade de compartilhamento de informações com terceiros, sendo que, quando houver exigência legal o sigilo deve ser preservado.
g. **Análise de vulnerabilidades**: Periodicamente, devem ser realizados testes para detecção de vulnerabilidades técnicas, incluindo-se aqui, todas as medidas necessárias para correção, incluindo a instalação de patches de correção, ou contenção das vulnerabilidades encontradas na análise.

É presente a resistência da implementação por privacidade como padrão nos sistemas informatizados, se baseando principalmente na dificuldade dos usuários, em caso de esquecimentos de senhas ou outros mecanismos que limitem o acesso de terceiros, como autenticação de dois fatores, por exemplo. Tradicionalmente a implementação por privacidade seria obtida a partir de outras funcionalidades sendo associadas a falsas dicotomias como a “privacidade x usabilidade”, “privacidade x funcionalidade”, “privacidade x benefício para o negócio” e até mesmo “privacidade x segurança” (AEPD, 2019).

O objetivo geral da implementação de todas as medidas administrativas e técnicas elencadas se baseia em boas práticas relacionadas à segurança da informação e proteção dos dados, todas com o objeto maior de promover um ambiente organizacional estruturado e seguro quanto ao tratamento dos dados pessoais, mas, nada impede que outras medidas e técnicas possam ser adotadas para maximizar a proteção necessária. De acordo com a LGPD, o responsável para auxiliar as entidades na implementação dessas medidas é o encarregado de dados.

3.1. Direitos dos usuários (titular dos dados pessoais)

Os titulares de dados pessoais, são as pessoas naturais que de alguma forma fornecem seus dados para terceiros em troca da utilização de algum serviço ou a realização de negócios e estes dados são objeto de tratamento. Os titulares em geral são a parte mais fraca na relação estabelecida com o controlador dos dados, sendo assim, para balancear essa relação, os titulares possuem direitos assegurados em relação a titularidade de seus dados, sendo garantidos os direitos a liberdade, intimidade e privacidades desses dados, tudo assegurado pela LGPD.

Dentre os direitos dos usuários, é necessária a informação das atividades de tratamento de dados pessoais, que deve ser executado de forma clara, transparente, considerando o respeito à privacidade, à intimidade, honra e imagem dos usuários, bem como às liberdades e garantias individuais, e outros princípios que exigem a proteção de dados pessoais, e deverão ser dispostos forma precisa e de acordo e a finalidade relacionada ao serviço prestado. Portanto, para atender ao princípio do livre acesso, o titular dos dados terá o direito de acessar facilmente as suas informações e obter dados sobre do tratamento de seus dados de forma adequada, ostensiva e facilmente acessíveis, incluídos aqui os agentes responsáveis pelo tratamento para atendimento, prevendo ainda, quando as decisões forem tomadas exclusivamente no tratamento automatizado, o direito de solicitar a revisão e o fornecimento todos os critérios utilizados na decisão automatizada, observando-se os segredos comerciais e industriais (CCGD, 2020).

A proteção da privacidade e intimidade são direitos fundamentais e necessitam de procedimentos para aplicação e atendimento a os princípios trazidos pela LGPD, assim, o respeito a privacidade, autodeterminação informativa, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico, além de princípios, são os principais objetivos da norma, sendo o consentimento para o tratamento dos dados deve estar

vinculados às finalidades específicas apresentadas (PINHEIRO, 2021).

Os titulares de dados ao fornecer seus dados pessoais, aceitando termos desproporcionais para utilização de serviços, virtuais ou não, podem sofrer maiores riscos em caso de ocorrência de incidentes de segurança e consequentemente vazamentos dos seus dados. A LGPD limita a necessidade do tratamento de dados ao necessário para execução das atividades empresariais, assim sendo, apenas aqueles dados que são estritamente necessários para a execução das atividades podem ser tratados. Ou seja, o tratamento de dados além do necessário extrapola os princípios da finalidade, da necessidade e da adequação, desta forma, em tese, é considerada ilegal e enseja a aplicação de multas e outras medidas administrativas pela ANPD.

O princípio finalidade por si, já pressupõem limitações e vinculação do tratamento dos dados coletados e armazenados a uma finalidade específica. Assim, tratamento de dados que de algum modo se sobressaia, como a venda direta de dados pessoais, que podem identificar um titular de dados, como a que era realizada pela empresa Serasa Experian[vii], que comercializava dados de pessoas físicas e jurídicas, como sexo, CPF, nome, endereço e até três números de telefones dos titulares de dados, sendo possível a possibilidade da utilização de filtros (sexo, idade, poder aquisitivo, classe social, localização, modelos de afinidade e triagem de risco), é ilegal, pois permiti o direcionamento a um público específico e identificável diretamente. Da forma comercializada, a venda direta de dados pessoais puros, fere os princípios da prevenção, por ser meio para ensejar o início de atividades ilícitas ou abusivas, como tentativas de roubos de identidade, dificuldade no que se relacionado aos princípios da responsabilização e prestação de contas, sendo conduta desproporção, consequentemente ilícita, não suprida pelo consentimento do titular ou tratamento baseado no legítimo interesse do controlador.

A LGPD não proíbe a venda ou qualquer tipo de comercialização de dados, mas, traz limitação quanto ao tratamento direcionado ao consentimento do titular dos dados. Na venda

pura de dados pessoais de pessoas identificadas ou identificável, por não ser dados manifestamente públicos ou disponibilizados pelos titulares, a cessão onerosa ou não, não pode ser baseada em nenhuma hipótese de dispensa do consentimento, pois, fere princípios da LGPD, além da existência de limitações da cessão onerosa que o próprio código civil impõe com relação aos direitos da personalidade, a Constituição Federal, artigo 5º, inciso X, dispõe que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito de indenização pelo dano material ou moral decorrente de sua violação".

É evidente que os direitos dos titulares dos dados são assegurados pela LGPD, sendo o principal foco a tutela e proteção dos usuários de possíveis abusos na realização do tratamento de seus dados por qualquer agente de tratamento. Assim não, nos aprofundaremos nesse tema, mas, deixamos claro que os objetivos das implementações de todas as medidas administrativas e técnicas ligadas a TIC devem ser implementadas para demonstrar o cuidado do agente de tratamento com os dados dos titulares e para que no mínimo, seja atenuada a ocorrência de incidentes de segurança.

4. A LGPD e a aplicação das medidas técnicas e administrativas ligadas a TIC

A atuação da ANPD pode ser realizada de forma ativa e ostensiva, na medida em que pode solicitar os relatórios de impactos de tratamento de dados diretamente aos controladores dos dados pessoais, sendo medida de difícil implementação de maneira ampla em razão do grande volume de informações. Outra forma de atuação da ANPD é a realizada de forma reativa, a partir de denúncias e reclamações realizadas que são recebidas pelo órgão e a auto declaração da entidade empresarial, por meio do controlador, em ocorrendo algum incidente de segurança[viii] da informação que implicarem de alguma forma na não conformidade com a LGPD, como no caso de vazamento ou manipulação de dados.

As medidas técnicas de segurança devem ser implementadas para promover a adequação

entre LGPD e a proteção necessária aos dados pessoais, promovendo um ambiente seguro, direito de todos os usuários. Assim sendo, é recomendado a utilização de framework, boas práticas ou normas técnicas como a ABNT NBR ISO/IEC 27001; ABNT NBR ISO/IEC 27002; Extensão da ABNT NBR ISO/ IEC 27001 e ABNT NBR ISO/IEC 27002; ISO/IEC 29151; CIS® (Center for Internet Security, Inc.®) Controls™ e ISO/IEC 29134 (CCGD, 2020).

É fato que a aplicação da LGPD na sua totalidade em microempresas, empresas de pequeno porte e startups, as denominadas de agentes de tratamento de pequeno porte, pode inviabilizar as suas atividades em razão dos controles exigidos e necessários à segurança da informação, como as exigidas para os meios digitais. É tamanha a preocupação, que a lei já tem a previsão de procedimentos simplificados e diferenciados para esses agentes. A ANPD, vem buscando mecanismos para que os agentes de pequeno porte realizem o tratamento diferenciado e tenham o tratamento adequado em relação a aplicação da LGPD, como é evidente no Guia Orientativo Segurança da Informação para Agentes de Tratamento de Pequeno Porte, que tem o objetivo de disseminar boas práticas e medidas básicas de segurança da informação para o tratamento de dados pessoais, tornando o ecossistema de proteção de dados pessoais mais seguro, apresenta medidas administrativas que envolvem a política de segurança da informação relacionada a dados pessoais e a segurança em recursos humanos e medidas técnicas, que tratam do controle de acesso aos dados; da segurança nos dados armazenados; da manutenção de programa de gerenciamento de vulnerabilidades; e da segurança das comunicações. Este guia contribui para estabelecer um ecossistema de proteção de dados pessoais mais seguro e, consequentemente, para um aumento na confiança dos usuários nos agentes de tratamento de pequeno porte. Nesse sentido, o guia orienta a implementação de uma POSIN para esse nicho de entidades empresariais, possibilitando assim, o planejamento, a implementação e o controle de ações relacionadas à segurança da informação, que embora não seja obrigatória, são incentivadas pela ANPD aos agentes de tratamento de pequeno porte, pois evidenciam a boa-fé, a diligência e cuidado para alcançar a segurança dos dados pessoais sob sua custódia e fornecem as diretrizes para

a gestão da segurança da informação. O propósito fundamental da POSIN é ser uma ferramenta que apoie a implementação de um processo estruturado de segurança da informação adequado a cada organização, considerando seu negócio e seu porte, de forma que essas medidas representem menor custo para permitir que as empresas continuem competitivas (ANPD, 2021a).

Desde de a publicação pela ANPD, de minuta de resolução que versa a respeito a respeito de procedimentos simplificados para os agentes de tratamento de pequeno porte[ix] até a publicação da resolução CD/ANPD nº 2[x], destacamos algumas flexibilizações: a) Registro voluntário das operações de tratamento de dados pessoais; b) Relatório de Impacto à Proteção de Dados Pessoais (RIPD) simplificado; c) Possibilidade de dispensa, flexibilização e simplificação para comunicação de incidente de segurança, a ser regulamentada pela ANPD; d) Facultativo ao agente de tratamento para atendimento de requisição dos titulares de dados pessoais, a opção entre anonimizar, bloquear ou eliminação de dados que sejam desnecessários, coletados além do que necessário (excessivos) ou ainda, tratados em desconformidade com a LGPD; e) Prazo em dobro para atendimento das solicitações dos titulares de dados e comunicação de incidentes de segurança da informação a ANPD; f) Não obrigatoriedade na indicação de encarregado de dados; Dentre outros. A resolução representa grande avanço para as empresas de pequeno porte, pois permite a diminuição dos custos para implementação e manutenção da governança de dados, com o objetivo de que mais empresas se adequem às necessidades da segurança da informação. Por outro lado, a flexibilização pretendida, pode enfraquecer os controles da LGPD com relação a proteção de dados pessoais, para fomentar o desenvolvimento nacional das entidades de pequeno porte.

Observamos que as regras de flexibilização para os agentes de pequeno porte no tratamento de dados pessoais devem ser executados de forma clara, transparente, considerando o respeito à privacidade, à intimidade, honra e imagem dos usuários, bem como às liberdades e garantias individuais, e outros princípios que exigem a proteção de dados pessoais. Assim,

não devem influenciar na autodeterminação informativa, nas liberdades de desenvolvimento da própria personalidade do titular dos dados e influenciar na liberdade de pensamento e tomada de decisão livre de qualquer influência de terceiros.

5. LGPD, suas sanções administrativas e a Legislação penal

A LGPD regula sanções apenas no âmbito administrativo que incluem advertência, multa, tornar pública a infração apurada e confirma a sua ocorrência, o bloqueio e a eliminação de dados pessoais, a suspensão e proibição total ou parcial das atividades de tratamento de dados pessoais que serão aplicadas de forma gradativa, isolada ou cumulativa de acordo com o caso em concreto, sendo levados em consideração os direitos afetados, a gravidade e abrangência do dano, a cooperação e condição econômica do infrator, e verificada a adoção da implantação das boas práticas, das políticas de segurança da informação e governança de dados e a adoção de medidas proporcional de correção[xi]. Entretanto, as sanções previstas na aplicação da LGPD não são alternativas ou substituem a aplicação de outras sanções administrativas, cíveis ou penais, como as definidas, por exemplo, no Código de Defesa do Consumidor e em legislação específica, sendo obrigação da ANDP a comunicação das autoridades competentes de todas as infrações penais que tiver conhecimento.

Outro ponto importante de se observar é a competência específica da aplicação nas sanções administrativas trazidas pela LGPD (Art. 52 – LGPD), ao qual compete exclusivamente à ANPD, sendo que há prevalência das competências no referente a proteção de dados, no entanto, a própria legislação abre a possibilidade de flexibilização quanto a articulação com outros órgãos e entidades com competências similares, sancionatórios e normativas, afetadas no tema de proteção de dados, sendo a ANPD o órgão responsável e central na interpretação e estabelecimento de normas e outras diretrizes para a aplicação e implementação da LGPD.

A ANDP, quanto à aplicação da legislação penal, como já mencionado, cabe apenas

comunicar às autoridades competentes todas as infrações penais que tiver conhecimento. Abaixo listamos os principais tipos penais que devem ser encaminhados às autoridades competentes para início da persecução penal.

a. Fraude eletrônica nos termos do Art. 171 do código penal, que foram acrescidos os parágrafos 2º A e B;
b. O Art. 153 do código penal inclui a divulgação, sem justa causa, de conteúdo de documento particular cuja divulgação possa produzir dano a outrem. É um crime condicionado à representação, quando não direcionada à administração pública. Sendo que a divulgação não autorizada de dados ou informação sigilosa contida em sistema, arquivo ou base de dados da administração pública, nos termos do art. 153, §1º-A do Código Penal;
c. Invasão de dispositivo informático, nos termos do art. 154-A do Código Penal, inclui a instalação de brechas ou outros para facilitar acesso de modo a se obter vantagem indevida, aumentando-se a pena se da invasão resultar prejuízos econômicos;
d. Furto qualificado por meio eletrônico nos termos do Art. os parágrafos 4º B e C do código penal;
e. Interrupção ou perturbação de serviço telemático ou de informação de utilidade pública, previsto no §1º do art. 266 do Código Penal;
f. Inserção ou facilitação de inserção de dados falsos, alteração ou exclusão de dados corretos nos sistemas informatizados ou bancos de dados da administração pública, nos termos do art. 313-A do Código Penal. Trata-se de crime próprio que só pode ser realizado por funcionário público;
g. Modificação ou alteração por funcionário público de sistema de informação ou programa de informática sem autorização, nos termos do art. 313-B do Código Penal. Trata-se de crime próprio que só pode ser realizado por funcionário público;

- Interceptação telemática clandestina, nos termos do art. 10 da Lei nº 9296/96.

A atuação da ANPD, quando tomar conhecimento de qualquer infração penal praticada no desempenho de suas funções e atividades realizadas, será a de comunicar às autoridades competentes, sendo suas atribuições específicas a aplicação das sanções administrativas trazidas nos termos da LGPD.

6. A necessidade de proteção e a visão mundial sobre os dados pessoais

Na execução das várias atividades sociais e econômicas a utilização de serviços on line é cada mais vez necessário no dia a dia de toda a sociedade. Muitos desses serviços têm seus negócios fortemente baseados no uso das tecnologias da informação, que naturalmente precisam realizar o tratamento de dados pessoais para concretização dos seus negócios. De acordo com a LGPD, os princípios da adequação e necessidade limitam o tratamento de dados pessoais ao mínimo necessários para alcance da finalidade da atividade, empresarial ou da própria administração pública, ou seja, fixa, mesmo que subjetivos, parâmetros limitadores para a realização do tratamento de dados, em sendo o caso concreto objeto de análise para se verificar a legalidade do tratamento. Por outro lado, qualquer serviço, embasado no legítimo interesse ou não, pode agir de forma maliciosa e ampliar o tratamento de dados para além do necessário, ampliando o conhecimento sobre seus usuários (titular dos dados pessoais), que ficam fragilizados em razão do grande número de informações que um serviço pode obter quando utilizado. Esses serviços podem obter informações como hábitos de viagem, de compras, e de alimentação, de atividades físicas e estilo de vida, tipos de notícias que são consumidas, atividade em sites e outros aplicativos, GPS, dados de sensores e qualquer outra informação que possa ser obtida aqui não mencionada. Entendemos que essa fragilidade ocorrida em razão de excessos no tratamento de dados pessoais é ilegal, mesmo que haja a tentativa de legalização por meio do consentimento dos usuários para a sua realização, pois, pode superar todos os limites que a finalidade empresarial possa necessitar, devendo ser analisado caso a caso. Para dificultar, muitas políticas de privacidade de serviços on-line são extensas, demandando tempo, paciência e energia para tentar analisar quais dados estão tratados e como eles serão utilizados. Essa

prática inibe o conhecimento da política de privacidade de um serviço em sua totalidade ao passo de um clique para o consentimento e acesso ao serviço.

O site security.org[xii] realizou a análise das políticas de privacidades de grandes empresas da área de tecnologia com o objetivo verificar quais os dados que grandes empresas de tecnologia como Facebook, Twitter, Amazon, Apple e Google têm dos usuários dos seus serviços. Nesse estudo, observou-se que a Google mantém uma grande coleção de registros dos usuários, enquanto a Apple só mantém os dados necessários para manter a conta dos seus serviços. Acredita-se que essa disparidade seja em razão dos negócios da Google, que é fortemente baseada em dados. Empresas como o Twitter e o Facebook mantêm mais informações que as necessárias para as suas atividades. Com relação ao Facebook, os dados obtidos são principalmente os inseridos pelo próprio usuário dos serviços. A Amazon se posiciona abaixo da Apple quando se trata de privacidade de dados. Observou-se que quanto maiores e robustos os negócios relacionados à publicidade, as entidades direcionam o tratamento de dados para se obter o maior conhecimento sobre os seus usuários. Acredita-se que empresas como a Google, Facebook e Twitter colecionam muitos dados dos usuários, além do necessário, para o direcionamento mais assertivo de campanhas de publicidade. Essa atitude pode representar grave ameaça à privacidade, o desrespeito às liberdades e garantias fundamentais que exigem a proteção de dados pessoais e dignidade das pessoas, sendo necessário a verificação caso a caso para se analisar a adequação legal.

Em sendo a proteção de dados pessoais um direito fundamental, sua proteção é de extrema importância, pois o respeito à privacidade e a proteção de dados pessoais são necessárias e vem sendo formalmente reconhecidas mundialmente por meio da instituição de leis de proteção de dados. A Figura 2 apresenta o levantamento realizado pela Conferência das Nações Unidas para o Comércio e Desenvolvimento (UNCTAD), que tem objetivo de apoiar os países em desenvolvimento de forma a proporcionar um ambiente justo e mais eficiente de integração na economia global, identifica que 128 de 194 países colocaram em prática legislação para garantir a proteção de dados e a privacidade, sendo em 67% dos países há

legislação para proteção e privacidade dos dados pessoais, em 10% há projetos de lei em tramitação para inclusão em seus ordenamentos jurídicos, enquanto, em 19% não há qualquer legislação e em 5% se quer dados ou registros a respeito de iniciativas nessa direção.

A proteção dos dados pessoais e privacidade é necessária e a LGPD, no caso brasileiro, fixa alguns parâmetros importantes para a sua aplicação e limitação do tratamento desses dados. Entendemos que o tratamento desproporcional de dados é ilegal e pode expor qualquer pessoa, causando além de danos financeiros, danos morais e a imagem. É evidente posição de fragilidade usuários (titulares de dados) frente os serviços digitais e a necessidade da sua proteção; exemplificamos alguns tipos de dados pessoais que podem ser obtidos quando o tratamento de dados desproporcional é realizado; levantou-se dados da análise das políticas de privacidades das principais grandes empresas de tecnologia analisada pelo site security.org, e a perspectiva mundial na implantação de leis relacionadas à privacidade e proteção de dados pessoais, deixando claro e evidente preocupação e movimentação na formalização legal da proteção da privacidade e dos dados pessoais.

7. CONSIDERAÇÕES FINAIS

Os dados pessoais são moedas de troca, quando não se paga por algum serviço no mundo digital, sendo grande as chances de a mercadoria ser os dados do próprio usuário, o titular dos dados, que dispõem seus dados pessoais, aceita termos de utilização desproporcionais, que divergem de uma finalidade legítima. Quanto maior a exposição de dados pessoais, maior os riscos de sofrer limitações ou influências relacionadas à autodeterminação e liberdades relacionadas ao desenvolvimento da própria personalidade e do pensamento, tudo em busca de vantagens econômicas das empresas que prestam esses serviços. Exemplo disso, é o algoritmo de ordenamento de posts “ranking de engajamento”, que organiza os posts de acordo com o que é de interesse do usuário, interesse este que é obtido a partir do seu próprio comportamento dentro de um serviço digital, e tem o objetivo de “prender” por

mais tempo a atenção do usuário. Neste exemplo fica evidente a violação à proteção dos dados pessoais, em especial a intimidade, o desrespeito à privacidade e a violação à autodeterminação informativa, tudo isso em busca do lucro.

A privacidade dos dados importa para todos. Assim sendo, é necessário o respeito às liberdades e garantias fundamentais que exigem a proteção de dados pessoais, e se relacionam diretamente com a privacidade, a intimidade, a honra e a dignidade. Nesse sentido, quanto mais se utiliza um serviço on line, seja gratuito ou não, trocando ou disponibilizando dados e informações, mais conhecimento sobre os interesses as plataformas possuirão dos usuários, desta forma, existe assim a possibilidade de influenciar na autodeterminação informativa, nas liberdades de desenvolvimento da própria personalidade do titular dos dados e influência na liberdade de pensamento que pode ser condicionada.

É evidente a posição de fragilidade dos usuários frente aos serviços digitais, sendo, por exemplo, muito difícil a comprovação de relação de causa entre dados vazados e o efetivo dano causado pela sua exposição, haja vista, que a exposição de dados obtidos por terceiros é realizada de forma ilícita e silenciosa. Os dados vazados são muitas vezes colocados à venda na *deepweb* ou distribuídos anonimamente, e como fator de complexidade, os agentes de tratamento podem sequer ter o conhecimento de que a sua base de dados foi exposta e está disponível na internet. Desta forma, até a origem dos dados vazados é difícil, e às vezes impossível, de identificar, sendo que parte da própria entidade que sofreu um incidente de segurança o dever de se auto denunciar a ANPD, indicar os titulares de dados afetados, o volume e os tipos de dados expostos e as medidas tomadas para atenuar o incidente, que são as medidas técnicas e administrativas ligadas a TIC. Sendo papel da ANPD proceder com as responsabilizações administrativas e comunicar às autoridades competentes os crimes que tiveram conhecimento no desempenho das suas atividades.

De um lado o fomento ao desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência, de outro lado o respeito a privacidade, a autodeterminação

informativa, as liberdades de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, todos estes fundamentos da LGPD que devem ser compatibilizados e harmonizados. Assim é imperioso que todo tratamento de dados seja balizado no respeito a legislação, na boa fé, bons costumes, de acordo com a ordem pública e função social de um instituto, visto que não agir com boa fé, implica por consequência que o tratamento realizado não será para finalidade legítima, por que não há legitimidade em tratamento que contraria a boa fé. Leis como a LGPD são marcos muito importantes na história da proteção dos dados pessoais, mas, os mecanismos legais como o tratamento de dados pessoais baseado no interesse legítimo certamente devem ser aperfeiçoados de forma a garantir o sigilo e a responsabilização de agentes que realizam tratamentos desnecessários e excessivos.

Todos os agentes que realizam o tratamento de dados por meio das TIC precisam implementar medidas administrativas e técnicas baseadas nas boas práticas relacionadas à segurança da informação e proteção de dados para evidenciar o zelo, o cuidado com os dados dos titulares e assim minimizar a ocorrência de falhas de segurança com o objetivo de garantir os direitos a liberdade, intimidade e privacidades dos dados pessoais dos usuários. As medidas administrativas e técnicas são necessárias e importantes no desenvolvimento de um ambiente organizacional estruturado e seguro para o tratamento dos dados pessoais, assim, devem ser obrigatoriamente colocadas em práticas pois, se tornam um direito dos usuários. Além das citadas neste trabalho, podem ser adotadas outras medidas técnicas para maximizar a proteção exigida. Observamos que existe flexibilização da aplicação das medidas técnicas e administrativas e a aplicação da LGPD na sua totalidade para os agentes de tratamento de pequeno porte, sendo previstos procedimentos simplificados e diferenciados para esses agentes. Desta forma, com o tratamento diferenciado, pretende-se não inviabilizar as atividades de agentes de pequeno porte. Porém, o tratamento realizado por esses agentes deve ser executado de forma clara, transparente, considerando o respeito à privacidade, à intimidade, honra e imagem dos usuários, bem como às liberdades e

garantias individuais, e outros princípios que exigem a proteção de dados pessoais.

A LGPD é fruto de um processo histórico em que a proteção da intimidade, da vida privada e da autodeterminação não viciada são direitos fundamentais e devem ser resguardados. Exemplo disso são as várias iniciativas legais implementadas e em implementação em todo o mundo com o objetivo de proteger os dados pessoais e a privacidade. No caso da LGPD, mecanismos como o tratamento de dados baseado no legítimo interesse devem ser aperfeiçoado, sendo o tratamento baseado nessas hipóteses analisado, fiscalizado e monitorado efetivamente pelas entidades responsáveis pela fiscalização da proteção de dados, para se evitar excesso no tratamento de dados pessoais e outras ilegalidades decorrente do uso desses dados face aos elevados riscos para os direitos e liberdades dos usuários que não possam, ser atenuados com a implementação de medidas razoáveis com o uso da tecnologia. Reforçamos, que é responsabilidade das entidades, públicas ou não, a implementação de um ambiente seguro para atenuar eventuais falhas de segurança, a realização do tratamento de dados apenas do necessário para execução das atividades institucionais, a instituição de políticas de privacidade em linguagem mais acessível para os usuários dos serviços e outros esforços para assegurar os direitos e a proteção dos usuários para que tenham acesso facilitado às informações sobre o tratamento de forma adequada e ostensiva.

8. REFERÊNCIAS BIBLIOGRÁFICAS

AEPD – Agência Espanhola de Proteção de Dados. **A Guide to Privacy by Design.** Outubro de 2019, p. 8-9. Disponível em: https://www.aepd.es/es/documento/guia-privacidad-desde-diseno_en.pdf. Acesso em: 10 junho 2022.

ANPD. **Guia Orientativo Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Versão 1.0. 2021a. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>. Acesso em: 01

junho 2021.

ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Maio de 2021b. Disponível em <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf>. Acesso em: 28 julho 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019, p. 108.

BRASIL**,** Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD**). Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm >. Acesso em: 28 maio. 2021.

CCGD – COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. **Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD)**. Versão 2.0. Agosto de 2020. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dado s/guias/guia_lgpd.pdf >. Acesso em: 04 setembro 2021.

CCGD – COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. **Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos**. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) Versão 1.2 Brasília, setembro de 2021a. Disponível em: < https://www.gov.br/go ver nodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_tupp.pdf >. Acesso em setembro 2021.

CCGD – COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. **Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade** LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) Versão 2.0. Brasília, março de 2021b. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/gu ias/g

uia_requisitos_obrigacoes.pdf >. Acesso em agosto 2021.

CCGD – COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. **Guia de Elaboração de Inventário de Dados Pessoais** LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) Versão 1.1 Brasília, abril de 2021c. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf >. Acesso em agosto 2021.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet**. Fascículo Vazamento de Dados, [2021]. Disponível em: <https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf >. Acesso em agosto de 2021.

MAYER-SCHÖNBERGER, Viktor. "**Generational Development of Data Protection in Europe.**" In Technology and Privacy: The New Landscape, Eds. Agre, Phillip E. and Marc Rotenberg. Cambridge, MA: The MIT Press. 219-242, 1997.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. **Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018**. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters, 2019.

PARLAMENTO EUROPEU, **Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados –**

GDPR). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em: 25 maio. 2021.

PINHEIRO, Patrícia Peck, **Proteção de Dados Pessoais,** comentários a Lei nº. 13.709/2018 (LGPD), 3ª Edição. São Pauto Saraiva, 2021.

WEILL, P.; ROSS, J. **Governança de TI: Tecnologia da Informação**. São Paulo: Makron Books, 2006.

---

[i] Especialista em Direito e Processo Administrativo, Discente do Curso de Especialização em Lei Geral de Proteção de Dados Pessoais – LGPD da Faculdade LEGALE E-mail: lenardu@gmail.com.

[ii] Advogada, Analista Judiciária pelo Poder Judiciário do Estado de Mato Grosso – TJMT Pós Graduada em Direito e Processo Administrativo no Setor Público. E-mail: carolnlopes@gmail.com.

[iii] Disponível em: <https://www.un.org/development/desa/pd/sites/www.un.org.development. desa pd/files/wpp2022_summary_of_results.pdf>. Acesso em 20 de agosto de 2022.

[iv] Disponível em: <https://datareportal.com/reports/digital-2023-global-overview-report> Acesso em 20 de janeiro de 2023.

[v] Outros Guias relacionados aos aspectos operacionais de adequação à Segurança da informação e Proteção de Dados relacionados a LGPD podem ser obtidos na Secretaria de Governo Digital do Ministério da Economia. Segurança da Informação e Proteção de Dados. Disponível em: < https://www.gov.br

/governodigital/pt-br/seguranca-e-protecao-de-dados >. Acesso em 30 de outubro de 2021.

[vi] O art. 44, caput, LGPD, estabelece como parâmetros a inobservância da legislação e a segurança legitimamente esperada pelos titulares.

[vii] Para outras informações veja TJ-DF. Agravo De Instrumento. Processo nº.: 0749765-29.2020.8.07.0000. Relator: Desembargador Cesar Laboissiere Loyola.

[viii] A ocorrência de qualquer incidente de segurança que possa acarretar risco ou dano aos titulares de dados, principalmente se relacionados a dados sensíveis ou indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, existindo potencial risco de ocorrência de danos materiais ou morais a terceiros ou o volume de dados e quantitativo de indivíduos afetados é importante, a comunicação de incidente de segurança deve ser realizada a ANPD e aos titulares dos dados, sendo o prazo a título indicativo de 2 (dois) dias úteis, contados do conhecimento do incidente. ANPD – Comunicação de incidentes de segurança. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/incidente-de- seguranca > Acesso em 18 de outubro de 2021.

[ix] Disponível em: < https://www.gov.br/participamaisbrasil/minuta-de-resolucao-para-aplicacao-da-lgpd-para-microempresas-e-empresas-de-pequeno-porte->. Acesso em 30 de agosto de 2021.

[x] Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27 -de-janeiro-de-2022-376562019>. Acesso em 20 de junho de 2022.

[xi] O Art. 52 da LGPD traz todas as sansão administrativas que podem ser aplidas pela ANPD. Outras orientações sobre a aplicação da LGPD podem ser obtidas em Perguntas Frequentes – ANPD (atualização outubro/2021). Disponível em: < https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#c1 >. Acesso em 20 de outubro de 2021.

[xii] Security.org. The Data Big Tech Companies Have On You. Atualizado em 23 de agosto de 2021. Disponível em: https://www.security.org/resources/data-tech -companies-have. Acesso em: 25 de novembro 2021.