UNIVERSIDADE FEDERAL DE UBERLÂNDIA

DÂMARIS SUELEN SILVA

O DIREITO À PRIVACIDADE DOS USUÁRIOS:

A delimitação da liberdade dos Agentes de tratamento de dados em face da necessidade de proteção dos titulares no meio virtual

Uberlândia

2023

DÂMARIS SUELEN SILVA

O DIREITO À PRIVACIDADE DOS USUÁRIOS:

A delimitação da liberdade dos Agentes de tratamento de dados em face da necessidade de proteção dos titulares no meio virtual

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito Professor Jacy de Assis como requisito parcial para a conclusão do Curso de Direito.
Professor Orientador: Almir Garcia Fernandes

Uberlândia

2023

DÂMARIS SUELEN SILVA

O DIREITO À PRIVACIDADE DOS USUÁRIOS:

A delimitação da liberdade dos Agentes de tratamento de dados em face da necessidade de proteção dos titulares no meio virtual

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito Professor Jacy de Assis como requisito para a conclusão do Curso de Direito.
Professor Orientador: Almir Garcia Fernandes

Uberlândia, 2023.

Banca Examinadora:

_____

Professor Almir Garcia Fernandes – UFU (Orientador)

_____

Professora Keila Pacheco Ferreira – UFU (Avaliadora)

_____

Doutorando José Luiz de Moura Faleiros Júnior - USP/UFMG (Avaliador)

RESUMO

A sociedade atual está em constante desenvolvimento, seja em áreas do conhecimento, nas relações entre os indivíduos, no modo de convívio das pessoas, bem como na tecnologia. É fato que, os conhecimentos tecnológicos do século passado já não são os mesmos do século atual, e podemos contar atualmente com diversas descobertas e desenvolvimento de sistemas antes não utilizados, ou pouco desenvolvidos até então. Possuímos hoje programas e sistemas que fazem a vida das pessoas bem mais cômoda e prática, seja no momento de realizar compras, pagar uma conta, conversar com amigos e conhecidos, entre várias outras atividades. E é nesta sociedade altamente tecnológica que surge o embate analisado neste presente trabalho: A necessidade de coleta de informações por parte das pessoas jurídicas para que consigam prestar um serviço eficiente e a privacidade do usuário. Existe ainda, um limite claro entre o direito de informação das pessoas jurídicas e o direito à privacidade do usuário no meio virtual? E se não existe um limite para tais direitos, como pode o usuário ter um mínimo de proteção de sua privacidade? Tendo em vista que pode ser considerado a parte vulnerável da relação analisada. Com uma análise nas diversas Leis atualmente vigentes e em várias orientações por Órgãos regulamentadores, como a ANPD - Autoridade Nacional de Proteção de Dados, encontram-se algumas respostas para a questão. O presente trabalho possui como base para sua pesquisa doutrinas sobre o tema proteção de dados e privacidade, guias orientativos e análise de casos reais.

Palavras Chave: Privacidade, Liberdade de informação, Proteção, Limites, Intimidade.

ABSTRACT

Today's society is constantly developing, whether in areas of knowledge, in relationships between individuals, in the way people live together, or in technology. It is a fact that the technological knowledge of the last century is no longer the same as that of the current century, and we can now count on various discoveries and the development of systems that were previously unused or underdeveloped. Today we have programs and systems that make people's lives much more comfortable and practical, whether it's shopping, paying a bill, chatting with friends and acquaintances, among many other activities. And it is in this highly technological society that the clash analyzed in this paper arises: the need for legal entities to collect information in order to provide an efficient service and the privacy of the user. Is there a clear limit between legal entities' right to information and the user's right to privacy in the virtual environment? And if there is no limit to these rights, how can users have a minimum level of protection for their privacy? Given that they can be considered the vulnerable party in the relationship analyzed. An analysis of the various laws currently in force and various guidelines issued by regulatory bodies, such as the ANPD - National Data Protection Authority, provides some answers to this question. This work is based on doctrines on the subject of data protection and privacy, guidelines and analysis of real cases.

Key words: Privacy, Freedom of information, Protection, Limits, Intimacy.

SUMÁRIO

INTRODUÇÃO

O presente trabalho se dedica à análise e estudo da problemática que surge ao se analisar a delimitação de dois direitos previstos em Legislação: Direito à privacidade dos usuários e o direito à liberdade de informação da pessoa jurídica, com fim de prestar serviços e concretizar seu legítimo interesse, sendo esse conflito estudado tendo como base o meio virtual.

Inicialmente, vale salientar que o direito à privacidade é um direito fundamental estabelecido pela própria Constituição Federal em seu Artigo 5º, inciso X, ao dispor que são invioláveis: a intimidade, a vida privada, a honra e a imagem das pessoas, podendo inclusive o prejudicado ser indenizado por dano material ou moral advindos da violação.[1]

O tema privacidade por muito tempo foi estudado e discutido, e apesar de não possuir uma definição única, pode-se citar, de forma exemplificativa, o conceito dado por Nathalia Masson, sendo o de que a privacidade representa a plena autonomia do indivíduo em reger sua vida do modo que entender melhor, mantendo em seu exclusivo controle as informações atinentes à sua vida doméstica, aos seus hábitos, escolhas, segredos, entre outros, sem se submeter ao crivo da opinião alheia.[2]

Já Ingo Wolfgang Sarlet sustenta, de um modo subjetivo, que privacidade pode ser entendida como o direito de defesa ou à não intervenção por parte do Estado e de terceiros no respectivo âmbito de proteção do direito, bem como, o direito a não ser impedido de levar sua vida privada conforme preferir e de dispor livremente das informações sobre os aspectos que dizem respeito ao domínio da vida pessoal e que não interferem em direitos de terceiro.[3]

Portanto, tendo em vista a existência de diferentes conceituações do termo privacidade pode-se concluir que o direito resguardado pela Constituição Federal diz respeito à possibilidade do usuário decidir como, quando e de que forma dispor de suas informações e dados, escolher quando e o que receber, se poderá ser contatado, entre outras diversas possibilidades de intervenção de terceiros em sua vida pessoal.

É adequado mencionar que a Lei 13.709 de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados, tem como fundamento, previsto em seu Artigo 2º, o respeito à privacidade. Vale lembrar ainda que, a Lei Geral de Proteção de Dados - LGPD, abarca a

---

[1] BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidente da República, [2016]

[2] MASSON, Nathalia. Manual de Direito Constitucional. 4ª. ed. rev. atual. e aum. [*S. l.*]: Juspodivm, 2016.

[3] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Curso de Direito Constitucional. [*S. l.*: *s. n.*], 2017.

proteção de dados não apenas no âmbito físico, mas também no meio virtual, que será o objeto do presente trabalho.

Por outro lado, não se pode ignorar que, na sociedade atual, muitas atividades e serviços dependem necessariamente de dados e informações pessoais dos requerentes. Não é possível, por exemplo, que uma empresa confeccione um contrato com seu cliente sem lhe solicitar os seus dados para a sua qualificação como parte contratual, ou que um funcionário seja contratado sem fornecer qualquer documento de identificação, carteira de trabalho, entre outros.

Por isso, não pode o titular, alegando o seu direito à privacidade, negar-se a fornecer seus dados pessoais e ainda assim conseguir que a atividade solicitada seja satisfatória. Isto é, em contrapartida ao direito à privacidade, as pessoas jurídicas possuem o direito à liberdade de expressão, de informação, de comunicação, ao desenvolvimento econômico e tecnológico e a livre iniciativa. [4]

E é neste embate entre o direito à privacidade do usuário e o direito à liberdade de expressão, de informação, de comunicação, desenvolvimento econômico e tecnológico e a livre iniciativa das pessoas jurídicas que nasce a problemática aqui analisada: Existe uma delimitação para qualquer um dos direitos citados?

Outro ponto de extrema relevância é a evidente desproporcionalidade das partes envolvidas no processo: o usuário e a pessoa jurídica, sendo essa última, na maior parte dos casos, detentora de conhecimento técnico, jurídico e financeiro em superação ao primeiro, como se nota na relação de consumo, disposta entre fornecedor e consumidor. Vale salientar, entretanto, que a relação aqui abordada não se restringe apenas à consumerista, mas também pode ser estendida à relação trabalhista, relação contratual, entre outras, em que se encontra em um polo o usuário pessoa física e no outro a pessoa jurídica.

Por fim, é imprescindível notar que a problemática analisada terá como plano de fundo o meio virtual, pautado pelo Direito Eletrônico e demais legislações, tais como o Marco Civil da Internet. É importante frisar, ademais, que o ambiente virtual possui suas especificidades que o meio físico nem sempre adota.

Mediante ao exposto, o objeto da presente pesquisa será analisar se há uma desproporcionalidade das partes na relação de tratamento de dados, a forma como a Legislação lida com essa diferença entre o titular de dados e os agentes, buscando o respeito a

---

[4] 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

todos os direitos do usuários, sem impedir que os agentes de tratamento realizem seu serviço, bem como se o meio virtual traz novos desafios, visto a sociedade estar lidando com uma tecnologia que impulsiona demasiadamente o acesso a dados e informações em questão de segundos.

1 CONCEITO DE PRIVACIDADE E PROTEÇÃO DE DADOS E SUAS INTERFERÊNCIAS NO MEIO VIRTUAL

A preocupação com a privacidade, segundo o autor Danilo Doneda, tem como objeto a busca por um isolamento, tranquilidade e refúgio. Também conhecida como o "direito a ser deixado só" em alguns momentos da história. O autor defende que a privacidade começou a ser uma grande preocupação da sociedade em seus primórdios marcados pelo individualismo egoísta, sendo definida como a ausência de comunicação entre um sujeito e os demais.[5]

Já para a doutrinadora Nathalia Masson, a privacidade representa a plena autonomia do indivíduo em reger sua vida do modo que entender melhor, mantendo em seu exclusivo controle as informações atinentes à sua vida doméstica, aos seus hábitos, escolhas, segredos, entre outros, sem se submeter ao crivo da opinião alheia.[6]

Outro ponto de extrema importância para se iniciar o pensamento sobre os direitos à privacidade, segundo o autor Danilo Doneda, é que o controle de informações sobre os indivíduos sempre foi um elemento essencial na definição de poderes dentro de uma sociedade, além de ter sido utilizado para poder gerar uma potencialização de um controle social exercido pelo Estado, sendo uma observação do autor no sentido de que não é por acaso que, o controle de informações é uma característica comum entre os regimes totalitários.[7]

A partir desta ideia da potencialização do controle social do Estado através das informações dos indivíduos sob seu controle, pode se pensar sobre a mesma perspectiva pelo lado do setor privado, tendo em vista que este não possui um dever de transparência tão grande como o do Governo. Portanto, quanto controle poderiam ter as instituições privadas em contato com um número grande de informações dos usuários ligados ou não à elas?

De acordo com o livro de Danilo Doneda, o direito à privacidade não gira mais em torno do eixo pessoa, informação e segredo, tido como a não interferência entre os sujeitos, e sim em torno do eixo pessoa, informação, circulação, controle.[8]

Com base nesta problemática, já não basta apenas pensar no direito de não interferência do Estado ou demais indivíduos na vida privada das pessoas, tida como o direito à privacidade, sendo esta uma liberdade negativa, de não fazer dos indivíduos, a não invasão na esfera privada do indivíduo, mas urge a necessidade da criação de uma regulamentação para além da não interferência, sendo esta uma liberdade positiva da sociedade: o direito à

[5] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.
[6] MASSON, Nathalia. Manual de Direito Constitucional. 4ª. ed. rev. atual. e aum. [S. l.]: Juspodivm, 2016.
[7] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.
[8] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

proteção de dados, que visa um tratamento regulamentado deste dados, garantindo direito aos titulares, uma autodeterminação informativa, medidas de transparência, entre outros.

Isto é, a proteção de dados não abrange apenas a privacidade das informações, mas também o controle indevido desses dados e uma proteção contra qualquer tipo de discriminação ou preconceito, infringindo a própria liberdade pessoal.

A própria Lei Geral de Proteção de Dados traz como seus fundamentos o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.[9]

Ou seja, a Lei que disciplina o tratamento dos dados pessoais, tanto no âmbito virtual como no físico, tem como fundamento direitos relacionados com a defesa dos titulares cujos dados estão sendo tratados, não permitindo que sua privacidade e sua dignidade sejam atingidas, bem como fundamentos que resguardam a utilização destes mesmos dados aos agentes de tratamento, figuras que serão estudadas mais profundamente em capítulos futuros. Tais como, o direito à liberdade de expressão, da informação, o desenvolvimento econômico, tecnológico e de inovação, a livre iniciativa e a livre concorrência.

Portanto, o tratamento de dados pessoais não diz respeito à uma não invasão ao núcleo de privacidade do titular, pelo contrário, a Lei Geral de Proteção de Dados, assim como demais Leis no tocante ao tema, buscam regulamentar o uso devido destes dados, permitindo assim que agentes de tratamento, em sua grande maioria, empresas, tratem dados de forma correta, segura, transparente e respeitando todos os direitos dos titulares, evitando que este tratamento acabe se tornando uma transgressão aos direitos de privacidade e dignidade humana.

Ademais, há de se falar sobre o meio virtual, através do qual houve um grande impulso para a divulgação de informações e dados em questão de segundos, podendo inclusive alcançar grande parte do mundo, segundo o autor Danilo Donela:

> O surgimento da rede Internet, por exemplo, decididamente alargou as possibilidades de comunicação e fez emergir um grande número de questões ligadas à privacidade. O impacto que esta rede representa, porém, estava em grande parte já incubado em outras tecnologias anteriores, que provocaram

[9] 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

> fenômenos em certa medida comparáveis e que, se hoje parece pálidos, devem ser considerados em relação ao que representaram à sua época.[10]

Isto é, a privacidade, que antes era entendida apenas como o direito de ser deixado só, atualmente, com a modernização e globalização consegue desenvolver um novo conceito, sendo relacionada ao grande fluxo de informações e condicionada à tecnologia desenvolvida. No mundo atual, uma informação vazada pelo meio virtual pode acarretar prejuízos irreversíveis, visto o alcance da rede de internet.

Ainda segundo Danilo Donela[11], atualmente, a invasão à privacidade se dá com maior frequência por meio da divulgação dos seus dados pessoais, pois, somos cada vez mais identificados a partir deles, sendo estes coletados de diversos meios.

Por fim, é importante salientar que, a proteção de dados, assim como a privacidade é prevista em nosso ordenamento, não só através da Lei Geral de proteção de dados, mas, segundo o autor Bruno Ricardo Bioni, a proteção de dados deve ser reconhecida como um novo direito da personalidade, além dos previstos no Código Civil nos artigos 11 a 21.[12]

[10] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.
[11] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.
[12] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3ª. ed. rev. atual. e aum. [S. l.: s. n.], 2021.

2 AGENTES DE TRATAMENTO E RESPONSABILIDADE CIVIL DO AGENTE

Para que se possa entender a definição do que são os agentes de tratamento, é preciso que se conheça a definição de tratamento de dados. A Lei Geral de Proteção de Dados define-o como toda operação realizada com dados pessoais, como as 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;[13]

Portanto, o tratamento de dados em uma relação de prestação de serviços ou comercialização de algum produto por uma pessoa jurídica, pode ser caracterizado no ato de coleta de qualquer dado, no seu armazenamento, compartilhamento, entre outros processos.

Com base nisto, pode-se entender que o agente de tratamento de dados é a figura responsável por esse armazenamento, compartilhamento e processamento das mais diversas informações coletadas.

Esses agentes são classificados em controladores, operadores, sub operadores, controladores conjuntos, entre outros diversos. Para efeitos da presente pesquisa, será analisado o conceito apenas de operador e controlador, conforme o Guia Orientativo da ANPD - Autoridade Nacional de Proteção de Dados:

> São agentes de tratamento o **controlador e o operador** de dados pessoais, os quais podem ser pessoas naturais ou jurídicas, de direito público ou privado. Ressalta-se que os agentes de tratamento devem ser definidos a partir de seu caráter institucional. Mas, além disso, o agente de tratamento é definido para cada operação de tratamento de dados pessoais, portanto, a mesma organização poderá ser controladora e operadora, de acordo com sua atuação em diferentes operações de tratamento.
> O **controlador** é o agente responsável por tomar as principais decisões referentes ao
> tratamento de dados pessoais e por definir a finalidade deste tratamento. Entre essas decisões incluem-se as instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais.
> O **operador** é o agente responsável por realizar o tratamento de dados em nome do
> controlador e conforme a finalidade por este delimitada.
> O operador só poderá tratar os dados para a finalidade previamente estabelecida pelo controlador. Isso demonstra a principal diferença entre o

[13] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 13 set. 2023.

> controlador e operador, qual seja, o poder de decisão: o operador só pode agir no limite das finalidades determinadas pelo controlador.[14]

Isto é, os controladores são aqueles que ditarão como o processo de tratamento de dados ocorrerá no caso concreto: quais dados serão coletados, se serão armazenados, para quais finalidades e quando serão descartados.E em decorrência desta possibilidade de tomada de decisões por parte do controlador, o mesmo também será responsável por todo e qualquer incidente e dano causado.

Já os operadores, nem sempre existirão. Eles participam do tratamento de dados quando são contratados pelos controladores, ou por algum outro motivo participam do processo que envolve esses dados, como, por exemplo, cumprimento de alguma obrigação legal. Isto é, por exemplo, uma empresa que coleta dados dos seus clientes para envio de mensagem de publicidade, pode ser considerada como controladora da relação. Entretanto, caso esta primeira empresa contrate outra empresa para elaborar a arte das mensagens publicitárias e realizar o envio aos seus clientes, esta segunda empresa será considerada como operadora, já que segue as regras impostas pela empresa colaboradora.

Por isso, por serem agentes que apenas tratam os dados em nome dos controladores, os operadores serão responsáveis em casos em que não estejam em conformidade com suas obrigações, estipuladas pelos controladores ou pela própria Legislação.

E conforme previsto pelo Guia Orientativo desenvolvido pela ANPD, as funções de controlador e operador irão depender de cada operação analisada, ou seja, uma empresa que em um processo é operadora, poderá ser controladora em outra.

Esta diferenciação de controlador e operador se faz necessária tendo em vista a responsabilização de cada um em casos de incidentes, danos, prejuízos, entre outros, já que o controlador possui uma responsabilidade maior que o operador no tratamento de dados, porque é ele quem ditará as normas e regras para o tratamento, logo, deverá observar o que é melhor para cada caso.

Segundo o Guia Orientativo da ANPD, pode se perceber essa diferenciação, pois:

> A LGPD atribui obrigações específicas ao controlador, como a de elaborar relatório de impacto à proteção de dados pessoais (art. 38), a de comprovar que o consentimento obtido do titular atende às exigências legais (art. 8º, § 2º) e a de comunicar à ANPD a ocorrência de incidentes de segurança (art. 48). Além disso, a atribuição de responsabilidades em relação à reparação

[14] GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO. 2. [S. l.], 1 abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em: 13 set. 2023.

> por danos decorrentes de atos ilícitos é distinta de acordo com a qualificação do agente de tratamento, isto é, se controlador ou operador, conforme o disposto nos arts. 42 a 45.
> Vale mencionar ainda que os direitos dos titulares (art. 18) são, em regra, exercidos em face do controlador, a quem compete, entre outras providências, fornecer informações relativas ao tratamento, assegurar a correção e a eliminação de dados pessoais, e receber requerimento de oposição a tratamento. O titular dos dados pode, ainda, peticionar contra o controlador perante a ANPD, o que denota a relevância da compreensão do conceito não só para os profissionais da área, mas também para o cidadão comum[15]

Esta responsabilização dos agentes de tratamento está disposta no artigo 42 da Lei Geral de Proteção de Dados, a qual diz que o controlador ou operador, que em razão do tratamento de dados que exerce causar danos em violação a legislação de proteção de dados é obrigado a repará-lo.[16]

Entretanto, com a Lei Geral de proteção de dados, ampliaram-se as discussões sobre esta responsabilidade dos agentes de tratamento, sendo analisado se a responsabilidade a eles atribuída seria uma responsabilidade objetiva, independente de culpa, ou se se trataria de uma responsabilidade subjetiva.

Para Bruno Bioni e Daniel Dias, o mais importante não está na classificação da responsabilidade em objetiva ou subjetiva, mas realizar uma análise em detalhes sobre os elementos normativos que restringiriam ou alargariam a discussão da culpabilidade para fins de responsabilização dos agentes.Ainda, segundo os autores:

> A primeira versão do então anteprojeto de lei de proteção de dados pessoais, bem como a proposta legislativa do Senado Federal expressamente adotavam um regime de responsabilidade civil objetiva. Enquanto a primeira preceituava que "o tratamento de dados [seria] uma atividade de risco", a segunda estabelecia que os agentes da cadeia responderiam, "independentemente da existência de culpa", pela reparação dos danos. A partir da segunda versão do anteprojeto de lei, ganhou força a opção por um regime de responsabilidade civil subjetiva. Apesar de ter sido amplamente criticada ao longo do segundo processo de consulta pública e em audiência pública realizada na Câmara dos Deputados, essa escolha foi a que prevaleceu no Congresso. A redação final da LGPD eliminou os termos antes aventados – "independentemente de culpa" ou "atividade de risco" – que eliminariam a culpa como um dos pressupostos da responsabilidade civil. [...]deve-se avançar para além da constatação binária de se o regime jurídico de responsabilidade civil da LGPD é de natureza objetiva e ou

[15] GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO. 2. [S. l.], 1 abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em: 13 set. 2023.

[16] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 13 set. 2023

> subjetiva. Isto porque, não deve haver dúvidas de que a política legislativa adotada exige a investigação em torno de um juízo de culpa dos agentes de tratamento de dados, mas, ao mesmo tempo, prescreve uma série de elementos com alto potencial de erosão dos filtros para que os agentes de tratamentos de dados sejam responsabilizados. Ainda que possa parecer paradoxal, o resultado pode ser um regime jurídico de responsabilidade civil subjetiva com uma espécie de alto grau de objetividade.[17]

Desse modo, considerando o entendimento de Bruno Bioni e Daniel Dias, conclui se que o regime de responsabilidade civil adotada pela LGPD é subjetivo.

Ademais, é de extrema importância citar as excludentes dessa responsabilidade dos agentes de tratamento, prevista no artigo 43 da Lei Geral de Proteção de dados, sendo elas observadas nos casos em que os agentes comprovarem que: (I) Não realizaram o tratamento de dados pessoais que lhes é atribuído; (II) Embora tenham realizado o tratamento de dados, não violaram a Legislação de proteção de dados; ou (III) O dano é decorrente de culpa exclusiva do titular de dados ou de um terceiro.[18]

O artigo 44 da mesma Lei ainda preceitua que o tratamento de dados será irregular quando deixar de observar a Legislação quanto à proteção de dados ou quando não fornecer a segurança que o titular de dados pode esperar, consideradas as circunstâncias. Não se tratando de qualquer expectativa de segurança, mas de expectativas juridicamente legítimas, assim como é adotado no Código de Defesa do Consumidor.[19]

Por fim, é importante salientar que, por se tratar de um regime de responsabilidade baseado em culpa do agente de tratamento, deve-se uma atenção maior ao princípio da *accountability*, isto é, uma forma de "prestação de contas" ou responsabilização[20], que acompanha os relatórios de impacto e o estímulo e reforço à capacidade dos agentes de tratamento de dados pessoais de auto-organização. A definição do princípio da *accountability* aponta para que haja juízo de valor em torno da conduta do agente de tratamento de dados para a sua responsabilização.[21]

---

[17] BIONI, Bruno; DIAS, Daniel. RESPONSABILIDADE CIVIL NA LGPD: construção do regime por meio de interações com o CDC. In: Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: BR Bioni Sociedade Individual de Advocacia, p. 394-495, 2021

[18] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 13 set. 2023

[19] BIONI, Bruno; DIAS, Daniel. RESPONSABILIDADE CIVIL NA LGPD: construção do regime por meio de interações com o CDC. In: Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: BR Bioni Sociedade Individual de Advocacia, p. 394-495, 2021

[20] LGPD: A aplicação da Lei Geral de Proteção de Dados pessoais no STJ. [S. l.], 4 maio 2022. Disponível em: https://www.stj.jus.br/sites/portalp/WebPub/NovoPortal/midias/cartilha-lgpd-novo.pdf. Acesso em: 6 out. 2023.

[21] BIONI, Bruno; DIAS, Daniel. RESPONSABILIDADE CIVIL NA LGPD: construção do regime por meio de interações com o CDC. In: Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: BR Bioni Sociedade Individual de Advocacia, p. 394-495, 2021

3 CONSENTIMENTO DO USUÁRIO E SUA VULNERABILIDADE

Inicialmente, vale ressaltar que, segundo Bruno Ricardo Bioni, a primeira geração de Leis relacionadas à proteção de dados surge com o processamento massivo de dados dos cidadãos, visando planejar e coordenar suas ações para um crescimento ordenado, fazendo com que alguns países cogitasse até mesmo a criação de bancos de dados unificados para a expansão orgânica da população, no Estado Moderno.[22]

Face ao receio quanto ao uso indevido dos dados e de uma invasão ao direito de privacidade, surgiu a necessidade de uma regulamentação do tratamento destes dados por meio de uma autorização para o seu funcionamento. Isto é, regularizar o uso da tecnologia, bem como dos bancos de dados, e com o passar do tempo, não somente na esfera governamental, mas também na privada.

Em um primeiro momento, o uso dos dados pessoais estava sob a responsabilidade da coleta de autorização do Estado, entretanto, percebe se a inviabilidade desta função, passando então a ser exercida pelo próprio titular de dados, fazendo-o por meio do seu consentimento, podendo este escolher como deverá ser o tratamento dos seus dados e informações pessoais.

Com base neste consentimento, que proporciona um maior controle do titular sobre os seus dados, deve se atentar à autodeterminação informacional, que de acordo com o autor Márcio Cots, pode ser entendida como o direito primeiramente de possuir informações necessárias sobre a tomada de decisões, bem como de controlar os seus dados pessoais, decidindo sobre como será coletado, transferências, acesso aos dados, correção, revogação de seu consentimento, entre outros.[23]

Atualmente, este consentimento é definido pela Lei Geral de Proteção de Dados como sendo a manifestação livre, informada e inequívoca pela qual o titular de dados concorda com o tratamento dos seus dados para uma finalidade determinada anteriormente pelo agente de tratamento.[24]

Isto é, caso algum agente de tratamento deseje manusear qualquer dado do titular com base no seu consentimento, ele deve se atentar para a adequada e específica coleta do consentimento, evitando que isso seja feito de forma genérica e ampla. O consentimento ainda deverá ser de forma livre, permitindo que o titular possa não consentir, caso deseje, de forma

[22] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. rev. atual. e aum. [S. l.: s. n.], 2020.
[23] COTS, Márcio; OLIVEIRA, Ricardo. Lei geral de proteção de dados pessoais comentada. 4. ed. rev. atual. e aum. [S. l.: s. n.], 2020.
[24] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 13 set. 2023

clara e informada, com todas as informações pertinentes para que entenda como se dará o tratamento e para qual finalidade, e por fim, de forma inequívoca, sem que o titular fique em dúvida para quais atividades estará consentindo.

Entretanto, com o avanço das tecnologias e principalmente dos sites e redes sociais, com os quais o titular possui contato diariamente, a coleta deste consentimento acaba se tornando um desafio, tanto para o agente de dados, que possui uma gama de usuários frequentando o seu site, bem como para os titulares, que nem sempre percebem que seus dados estão sendo tratados ou não notam que o seu consentimento foi coletado de forma errônea pelo site ou plataforma.

Com base nisto, pode-se constatar o quão vulnerável se torna o usuário, segundo Tarcísio Teixeira existe uma hipossuficiência do titular de dados pois em uma sociedade permeada pela cultura do *Big Data*[25], em que há uma coleta massiva de dados, o titular de dados se encontra em uma posição claramente desfavorável, sendo quase impossível saber quais de seus dados estão sendo tratados por aqueles agentes de tratamento.[26]

Além da falta de informações por parte dos titulares, de acordo com Bruno Bioni, o *Big Data* faz com que a base de dados levantada pelos agentes de tratamento possa servir para uma gama de finalidades, podendo ser utilizada para inferir uma série de prováveis acontecimentos e padrões de comportamentos dos usuários. O *Big Data* pode prever, por exemplo, crises financeiras, o rompimento de relacionamentos, com base em posts dos usuários, entre outros, fazendo com que cada vez mais os dados dos usuários dispersos pela rede digam muito sobre eles e quem os manipula sabe até mais sobre os usuários do que eles mesmos. [27]

> Essa capacidade de identificar os mais diversos padrões de comportamentos e prever a sua recorrência no futuro é uma verdadeira "mina de ouro" para a abordagem publicitária. Por isso, Big Data revolucionou a indústria publicitária, criando-se mais do que um rico retrato do consumidor em potencial. A figura translúcida do consumidor de vidro agora perpassa seus passos futuros.[28]

[25] Segundo Bruno Bioni em seu livro "Proteção de dados pessoais: a função e os limites do consentimento", o Big Data é uma tecnologia que permite que um volume descomunal de dados seja estruturado e analisado para uma gama indeterminada de finalidades. Ainda de acordo com o autor, milhares de bases de dados são criadas e, por vezes, agregadas a outras para identificar uma série de padrões de comportamentos dos usuários e inferir a sua recorrência no futuro, com base nos termos agregados de pesquisa de um buscador, por exemplo. Uma mesma base de dados pode servir para uma gama de finalidades, podendo ser reutilizada para inferir uma série de prováveis acontecimentos e padrões de comportamentos, devendo-se, apenas, redefinir o algoritmo para novos usos e correlações, sendo, portanto, flexível para as mais diversas finalidades.

[26] TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Responsabilidade e ressarcimento de danos por violação às regras previstas na LGPD: um cotejamento com o CDC. In: LIMA, Cíntia Rosa Pereira de (Coord.). Comentários à Lei Geral de Proteção de Dados. São Paulo: Almedina, 2020, p. 322.

[27] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. rev. atual. e aum. [S. l.: s. n.], 2020.

[28] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. rev. atual. e aum. [S. l.: s. n.], 2020.

Para ilustrar este controle de dados sendo utilizado para conhecimento do usuário e uma consequente manipulação de suas ações e escolhas, pode-se citar a pesquisa desenvolvida pela doutoranda Débora Franco Machado em seu Mestrado pela Universidade Federal do ABC, em que a mesma examinou as patentes e solicitações de patentes depositadas pela Facebook Inc. nos Estados Unidos durante o período de 2014 a 2018, identificando aproximadamente 4.000 registros. [29]

Em seguida, ela aprimorou a pesquisa para concentrar-se naquelas relacionadas exclusivamente à plataforma de mídia social, e selecionou 39 delas que tinham o potencial de influenciar o comportamento dos usuários. Dentre essas, cerca de 15% integravam a análise de emoções como um componente essencial de seu funcionamento.

Segundo Débora Machado, existem patentes que detectam emoções de uma pessoa ao acessar a sua rede social e através dessa análise direciona a esta pessoa postagens identificadas como adequadas para este sentimento. Além de direcionamento de postagens, as emoções analisadas também poderão ser utilizadas para apresentar propagandas aos usuários, conforme suas palavras:

> É o caso da patente US20150242679A1, Techniques for emotion detection and content delivery, que mostra uma funcionalidade capaz de detectar qual emoção uma pessoa está sentindo ao utilizar uma rede social e assim direcionar a ela postagens identificadas como adequadas para aquele tipo de sentimento. Como motivo para ter sido criada, o texto descreve o crescimento da quantidade de informação disponível ao usuário nas redes sociais online e o aumento do tempo que o usuário passa navegando entre notícias, vídeos e outros conteúdos digitais para encontrar algo que realmente o interesse. Ao mesmo tempo, a patente aponta que os sistemas de entrega de conteúdo ainda não utilizam informações de imagem passiva e, portanto, existe uma necessidade de uma solução de entrega de conteúdo que aproveite os dados de imagem passiva disponíveis para fornecer conteúdo com relevância aprimorada ao usuário.Segundo a patente, o sistema também pode ser útil para o mercado publicitário, pois o estado emocional do usuário poderá ser utilizado para apresentar propagandas, uma vez que a ferramenta consegue identificar quando o usuário está olhando para a tela do celular ou não. Assim, é possível solicitar que anúncios apareçam apenas quando o usuário estiver atento, ou que apareçam anúncios inspiradores quando ele estiver triste e anúncios interativos quando estiver entediado. [30]

[29] MODULAÇÕES ALGORÍTMICAS: uma análise das tecnologias de orientação de comportamento a partir das patentes do Facebook. 2019. Dissertação apresentada ao Programa de Pós Graduação em Ciências Humanas e Sociais da Universidade Federal do ABC (UFABC) (Ciências Humanas e Sociais) [S. l.], 2019. Disponível efile:///C:/Users/damar/Downloads/MODULACOESALGORITMICAS_dissertacaoDeboraMachado.pdf. Acesso em: 16 out. 2023.

[30] MODULAÇÕES ALGORÍTMICAS: uma análise das tecnologias de orientação de comportamento a partir das patentes do Facebook. 2019. Dissertação apresentada ao Programa de Pós Graduação em Ciências Humanas e Sociais da Universidade Federal do ABC (UFABC) (Ciências Humanas e Sociais) [S. l.], 2019. Disponível em:

Ainda segundo Débora Machado, em 2012, pesquisadores do Facebook, colaborando com acadêmicos da Universidade de Cornell, divulgaram uma pesquisa que se baseou em analisar as postagens que 689 mil usuários visualizaram em seus Feeds de Notícias. O estudo teve como objetivo investigar se as emoções expressas nas publicações dos amigos desses usuários na plataforma social tinham o poder de afetar o ânimo daqueles que as liam, potencialmente causando um fenômeno de "contágio emocional". [31]

De acordo com Débora, o experimento mostrou que o grupo que recebeu menos postagens positivas também publicou menos mensagens positivas em sua própria rede social, confirmando a hipótese de que os usuários ficam menos felizes após serem impactados por esse conjunto de mensagens com poucas palavras positivas. Nenhum dos usuários que teve seus *Feeds* de Notícias modificados foram informados sobre estarem participando de um estudo. A justificativa legal do Facebook é a de que, ao assinar os termos de uso da plataforma, todos os usuários aceitam participar de pesquisas e ter seus dados analisados.[32]

Portanto, segundo Bruno Bioni, com o avanço da ciência mercadológica, particularmente no que diz respeito à segmentação de produtos (marketing) e à promoção dos mesmos (publicidade), os dados pessoais dos cidadãos tornaram-se um elemento fundamental na máquina da economia da informação. A capacidade de organizar esses dados de forma altamente escalável por meio do *Big Data* deu origem a um novo mercado, cuja base repousa na extração e comercialização desses dados. Surge, assim, uma 'economia de vigilância' que tende a reduzir o cidadão a um mero espectador de suas próprias informações. Este diagnóstico é crucial, pois é a partir dele que podemos avançar na análise do papel do consentimento na proteção dos dados pessoais, especialmente quando se considera a passividade atribuída ao cidadão em relação ao fluxo de suas informações pessoais.[33]

Por isso, é de extrema importância que existam regulamentações e diretrizes para proteger o titular de dados, visto como parte vulnerável, tendo em vista não possuir todo o

---

file:///C:/Users/damar/Downloads/MODULACOESALGORITMICAS_dissertacaoDeboraMachado.pdf. Acesso em: 16 out. 2023.

[31] MODULAÇÕES ALGORÍTMICAS: uma análise das tecnologias de orientação de comportamento a partir das patentes do Facebook. 2019. Dissertação apresentada ao Programa de Pós Graduação em Ciências Humanas e Sociais da Universidade Federal do ABC (UFABC) (Ciências Humanas e Sociais) [S. l.], 2019. Disponível em: file:///C:/Users/damar/Downloads/MODULACOESALGORITMICAS_dissertacaoDeboraMachado.pdf. Acesso em: 16 out. 2023.

[32] MODULAÇÕES ALGORÍTMICAS: uma análise das tecnologias de orientação de comportamento a partir das patentes do Facebook. 2019. Dissertação apresentada ao Programa de Pós Graduação em Ciências Humanas e Sociais da Universidade Federal do ABC (UFABC) (Ciências Humanas e Sociais) [S. l.], 2019. Disponível em: file:///C:/Users/damar/Downloads/MODULACOESALGORITMICAS_dissertacaoDeboraMachado.pdf. Acesso em: 16 out. 2023.

[33] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. rev. atual. e aum. [S. l.: s. n.], 2020

controle sobre seus dados, tampouco das informações que podem ser extraídas e do tratamento executado através deles.

4 BASES LEGAIS NA LGPD E OS DIREITOS DOS TITULARES

Além do consentimento, existem algumas outras diversas bases legais pelas quais os agentes de tratamento podem manusear dados pessoais dos usuários. A Lei geral de proteção de dados traz dez hipóteses em que se é permitido realizar o tratamento de dados pessoais comuns, sendo essa a ressalva à regra de não tratamento de dados dos usuários.

O consentimento, já mencionado no capítulo anterior, é uma dessas dez hipóteses, sendo as demais no caso de cumprimento de obrigação legal ou regulatória pelo controlador; pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; para o exercício regular de direitos em processo judicial, administrativo ou arbitral; para a proteção da vida ou da incolumidade física do titular ou de terceiro; para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou para a proteção do crédito.[34]

Ou seja, para tratar os dados dos usuários em conformidade com a Lei Geral de Proteção de Dados é necessário que o tratamento se baseie-se em alguma das hipóteses elencadas no artigo 7º da mesma. Através das bases legais consegue-se regular como e em quais situações os agentes de tratamento poderão manusear os dados dos usuários, sem exceder-se ao razoável.

Ademais, é muito importante mencionar que nenhuma base legal é mais importante ou mais forte quando se trata de dados pessoais comuns[35], podendo o agente de tratamento utilizar a base legal que mais se adequa à situação concreta ou ao seu objetivo atual. Como por exemplo, uma empresa que pretende tratar os dados nome e email para envio de newsletters, poderá utilizar a base do legítimo interesse, caso o seu objetivo seja atingir um

[34] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 13 set. 2023

[35] CONTRACT. [S. l.], 18 out. 2023. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/contract/. Acesso em: 18 out. 2023.

número grande de usuários, mas se a empresa se preocupa mais com que os usuários que receberão a newsletter tenham realmente interesse no conteúdo que será enviado, a mesma poderá utilizar a base do consentimento, que poderá reduzir consideravelmente a lista de destinatários, mas todos os que estiverem nesta lista realmente gostariam de receber o conteúdo.

Isto é, cada atividade de tratamento de dados pessoais deve utilizar a base legal mais adequada às circunstâncias do caso concreto, podendo, inclusive, os agentes de tratamento se basear em mais de uma hipótese de tratamento para o mesmo dado, desde que, o mesmo seja utilizado para finalidades diferentes em diversos processos.

Em sua pesquisa, Renato Leite Monteiro e Sinuhe Cruz afirmam que uma das ferramentas destinadas a identificação da base legal mais adequada ao caso concreto é uma fórmula baseada em três elementos, sendo estes: a) A origem do dado tratado; b) O tipo de dado tratado e por fim c) A finalidade do tratamento do dado. Os três elementos, ao serem somados e com base nos princípios norteadores da Lei Geral de Proteção de Dados poderão auxiliar na definição da base legal adequada para a atividade de tratamento analisada.[36]

Por outro lado, é importante mencionar também, que dentre as bases legais listadas pela Lei Geral de Proteção de Dados, algumas são específicas de determinados segmentos ou agentes de tratamento. Tais como, a base legal para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, sendo esta utilizada apenas pela administração pública, já que as políticas públicas são de sua responsabilidade.

Ademais, a base legal da proteção à vida ou incolumidade física do titular ou de terceiro, bem como a base legal da tutela da saúde, que devem ser utilizadas exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

E por fim, tem se a base legal para a realização de estudos por órgão de pesquisa, podendo ser utilizada apenas por órgãos de pesquisa, sendo este definido pela Lei Geral de Proteção de Dados como um órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis

[36] DESAFIOS para a efetivação do direito à explicação na Lei Geral de Proteção de Dados no Brasil. 2021. Tese de doutorado (Direito) - Universidade de São Paulo, [S. l.], 2021. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2139/tde-22072022-120338/publico/8106861DIO.pdf. Acesso em: 19 out. 2023.

brasileiras, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.[37]

Portanto, as bases legais se tornaram hipóteses em que se entendeu que seria razoável que houvesse um tratamento de dados no caso concreto, seja porque o titular optou por acordar um contrato, porque consentiu com o tratamento, o agente está cumprindo ordens de algum órgão público, entre outros. Entretanto, vale lembrar que a Lei diz expressamente que somente poderá haver tratamento caso haja uma base legal que o fundamente. Logo, impede que os agentes de tratamento utilizem os dados dos titulares como desejarem sem qualquer restrição ou cuidado.

Outrossim, além da responsabilidade dos agentes de tratamento em manusear os dados coletados em face de uma das bases legais elencadas, hipóteses permissivas para o tratamento de dados dos titulares, a Lei Geral de Proteção de dados também enumera direitos garantidos aos titulares, em seu artigo 18, como uma outra forma de proteção da parte vulnerável da relação.

Entre os direitos dos titulares estão: confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei; portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; eliminação dos dados pessoais tratados com o consentimento do titular; informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; revogação do consentimento.

Os direitos dos titulares possuem a função de auxiliar no objetivo de transparência e prestação de contas dos agentes, pois permite que o titular tenha acesso aos dados que estão sendo tratados, quais as finalidades do tratamento, bem como permite que o titular possua voz ativa em relação aos seus dados, podendo, realizar a portabilidade desses dados, a revogação do consentimento, caso tenha o dado para o agente de tratamento, a eliminação dos dados coletados, entre outras possibilidades. Os princípios norteadores dos direitos dos titulares são

[37] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 13 set. 2023

o Princípio da finalidade[38], adequação[39], necessidade[40], livre acesso[41], qualidade dos dados[42], transparência[43], segurança[44], prevenção[45],
não discriminação[46] e da responsabilização e prestação de contas[47].

Ademais, é importante que o agente de tratamento disponibilize em local de fácil acesso ao seus usuários, um canal para que os mesmos possam solicitar os seus direitos. Inicialmente, não é necessário que a empresa tome providências imediatas quanto à solicitação, tendo em vista que em grande parte dos casos o agente de tratamento deverá analisar a viabilidade do pedido, as consequências do atendimento deste pedidos e os impactos para a empresa.

Por isso, a própria Lei Geral de Proteção de Dados aconselha que seja dada uma resposta ao titular de porquê a sua solicitação não será atendida imediatamente, como no caso

---

[38] Segundo o Guia de boas práticas, disponibilizado pela ANPD - Autoridade Nacional de proteção de Dados, no site do Governo Federal, o princípio da finalidade se caracteriza como: Direito ao tratamento adstrito aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

[39] Segundo o Guia de boas práticas, disponibilizado pela ANPD - Autoridade Nacional de proteção de Dados, no site do Governo Federal, o princípio da adequação se caracteriza como: Direito ao tratamento adequado compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

[40] Segundo o Guia de boas práticas, disponibilizado pela ANPD - Autoridade Nacional de proteção de Dados, no site do Governo Federal, o princípio da necessidade se caracteriza como: Direito à 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.

[41] Segundo o Guia de boas práticas, disponibilizado pela ANPD - Autoridade Nacional de proteção de Dados, no site do Governo Federal, o princípio do livre acesso se caracteriza como: Direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

[42] Segundo o Guia de boas práticas, disponibilizado pela ANPD - Autoridade Nacional de proteção de Dados, no site do Governo Federal, o princípio da qualidade dos dados se caracteriza como: Direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento.

[43] Segundo o Guia de boas práticas, disponibilizado pela ANPD - Autoridade Nacional de proteção de Dados, no site do Governo Federal, o princípio da transparência se caracteriza como: Direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

[44] Segundo o Guia de boas práticas, disponibilizado pela ANPD - Autoridade Nacional de proteção de Dados, no site do Governo Federal, o princípio da segurança se caracteriza como: Direito à segurança dos dados, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de 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.

[45] Segundo o Guia de boas práticas, disponibilizado pela ANPD - Autoridade Nacional de proteção de Dados, no site do Governo Federal, o princípio da prevenção se caracteriza como: Direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

[46] Segundo o Guia de boas práticas, disponibilizado pela ANPD - Autoridade Nacional de proteção de Dados, no site do Governo Federal, o princípio da não discriminação se caracteriza como: Direito de não ser discriminado de forma ilícita ou abusiva.

[47] Segundo o Guia de boas práticas, disponibilizado pela ANPD - Autoridade Nacional de proteção de Dados, no site do Governo Federal, o princípio da responsabilização e prestação de contas se caracteriza como: Direito de exigir a adequada responsabilização e a prestação de contas por parte dos agentes de tratamento, ao qual se contrapõe o dever, por parte destes, de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

da análise de viabilidade, bem como estabelecer um prazo para a resposta definitiva sobre a solicitação.[48]

Em casos em que a empresa entender que não será viável o atendimento da solicitação do titular de dados, como nos casos em que o titular solicitar a exclusão de seus dados, mas, a empresa necessita prestar contas à algum órgão governamental, o agente de tratamento deve informar de forma fundamentada a decisão ao titular, explicando lhe o motivo da recusa ao atendimento de seu pedido.

Por fim, é relevante mencionar que ao procurar o canal de solicitação dos direitos dos titulares, os titulares devem conseguir emitir o seu requerimento sem qualquer custo para isto, sendo o pedido finalizado nos prazos e termos estabelecidos em Lei e nos próprios regulamentos e políticas da empresa.

[48] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 13 set. 2023

5 PROGRAMA DE GOVERNANÇA

Além dos direitos e princípios que norteiam a proteção de dados, a Lei Geral de Proteção de Dados traz em seu artigo 50, Seção II - Das Boas Práticas e da Governança, a importância da observação dos princípios, ligados à estrutura, escala, volume das operações, a sensibilidade dos dados a probabilidade e a gravidade dos danos para os titulares, informando que o titular poderá implementar um programa de governança em privacidade como forma de adequação prática de todo o exposto na Lei.[49]

O programa de governança em privacidade pode ser compreendido como um programa que guiará a empresa para que ela busque a conformidade com as leis e regulamentações em relação à privacidade e proteção de dados, utilizando se de objetivos, metas, métodos e meios possíveis para isto.

A LGPD ainda afirma que este programa de governança deverá, no mínimo, demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; O programa deve, ainda, ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta. Ademais, deverá ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados.[50]

Outrossim, o programa de governança deve estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade, além de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular. Além disso, devem ser aplicados mecanismos de supervisão internos e externos, contando com planos de resposta a incidentes e remediação, e ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.[51]

Portanto, é importante pensar que, o programa de governança busca fazer com que a empresa demonstre comprometimento com as operações que desenvolve cotidianamente,

---

[49] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 13 set. 2023

[50] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 13 set. 2023

[51] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 13 set. 2023

além de ser baseado no princípio da transparência e na prestação de contas aos seus titulares de dados, estabelecendo assim um vínculo de confiança com seus clientes, colaboradores, parceiros e usuários externos.

Cada programa de governança, como exposto na Lei Geral de Proteção de Dados, deve se adaptar à estrutura da empresa, avaliando se tratar de uma empresa de grande porte ou uma pequena empresa, a escala e volume dos dados tratados, o quanto de dados diariamente são tratados em cada operação, e a sensibilidade destes dados, tendo em vista que a LGPD diferencia dados pessoais comuns de dados pessoais sensíveis, conforme definição em seu artigo 5º, inciso I e II:

> Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Portanto, inicialmente é de grande relevância que se estude a estrutura da empresa, as operações realizadas e as estratégias que serão adotadas. A partir disso, a empresa poderá criar diversas políticas, termos, regulamentos internos e externos que nortearão esse tratamento de dados, bem como trará clareza aos titulares sobre como o tratamento dos seus dados está sendo realizado.

Alguns exemplos dessas políticas e termos são as Políticas de privacidade interna (para os colaboradores) e externas (voltadas para os usuários e clientes da empresa), Política de segurança da informação, Planos de resposta à incidentes e Planos de resposta à solicitação dos titulares de dados, Política de governança de dados, entre outras diversas.

É importante mencionar que não basta apenas a confecção desses termos e políticas, mas também é de extrema importância que os colaboradores que exercem esses tratamentos de dados dentro da empresa entendam o que está em cada regulamento e sejam devidamente treinados e educados para lidar de forma correta e transparente, fazendo com que as políticas se tornem realidade no dia a dia da empresa.

Para facilitar o cumprimento das políticas e termos internos e externos, a empresa pode adotar a criação de um comitê interno, sendo este uma equipe que será responsável pela fiscalização e monitoramento das decisões quanto à proteção de dados.

O encarregado de dados, também denominado de *data protection officer - DPO*, definido no artigo 41 da LGPD, possui grande relevância para o programa de governança e adequação da empresa às diretrizes da Lei Geral de Proteção de Dados. Segundo o Guia

Orientativo da ANPD, o encarregado de dados pode desempenhar um importante papel de fomentar e disseminar a cultura da proteção de dados pessoais na organização, como, por exemplo, ao receber solicitações de titulares e da Autoridade Nacional de Proteção de Dados e adotar providências ou, ainda, ao orientar funcionários e contratados a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.[52]

Portanto, o programa de governança é uma das ferramentas que devem ser utilizadas para impedir que as orientações da Lei Geral de Proteção de dados se tornem apenas orientações vazias dispostas em uma Lei. Através do programa de governança a empresa pode de fato colocar em prática os princípios e normas norteadoras da proteção de dados, gerando confiança em seus titulares, trazendo a transparência necessária para o bom relacionamento empresa-cliente, além de ser uma das formas de demonstração de que a empresa de fato está cumprindo com o determinado na legislação, seja através de documentos, tais como políticas e termos, mas através de mecanismos de segurança, treinamento de seus colaboradores, entre outros.

[52] GUIA Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. 2. ed. [S. l.: s. n.], 2022. Disponível em: https://drive.google.com/file/d/1lGflXGOXambguB6T8ieEbHC9qNOLvTKR/view. Acesso em: 20 out. 2023.

6 BOAS PRÁTICAS E SEGURANÇA NO TRATAMENTO DOS DADOS

Além do Programa de Governança, a Lei Geral de Proteção de Dados ainda recomenda que as empresas adotem boas práticas em suas atividades empresariais, tendo em vista as condições de organização, regime de funcionamento, os procedimentos, reclamações e petições dos titulares, as normas de segurança, padrões técnicos, as obrigações envolvidas no tratamento de dados, ações educativas, mecanismos internos de supervisão e mitigação de riscos, entre outros.[53]

6.1 Riscos e análise de impacto

Uma boa prática para as empresas que tratam dados dos seus usuários é a análise dos riscos deste tratamento. Entender os impactos e as consequências dessa operação é de extrema importância para planejar meios e formas de evitar que um incidente de proteção de dados ocorra.

O risco pode ser entendido como sendo o efeito da incerteza nos objetivos, podendo ser expresso como uma combinação das consequências de um determinado evento e a probabilidade de sua ocorrência. A gestão desse risco seria a aplicação de políticas de gestão, procedimentos, atividades de comunicação, consultoria, estabelecimento de contexto, identificação, análise, avaliação, tratamento, monitoramento e revisão desses riscos.[54]

A Lei Geral de Proteção de Dados Pessoais aborda, em diversos trechos de seu texto, a menção ao perigo e à importância de examinar os potenciais resultados indesejados das atividades envolvendo dados pessoais. Isso é feito para verificar como tais atividades afetam os direitos e as liberdades individuais dos detentores dos dados.[55]

Para auxílio nesta tarefa, tem se a avaliação de impacto do tratamento de dados, definida por Dariusz Kloza como uma ferramenta usada para a análise de possíveis consequências e perigos que podem ser apresentados em face de um interesse social relevante.

---

[53] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 13 set. 2023

[54] ISO 27001: Curso completo para certificação EXIN ISFS!. [S. l.], 24 out. 2023. Disponível em: https://www.udemy.com/course/isfs-iso27001/. Acesso em: 24 out. 2023.

[55] GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

A avaliação possui o intuito de auxiliar no processo decisório, em relação a viabilidade do tratamento e sob quais condições, protegendo assim, os interesses sociais. [56]

De acordo com a Lei Geral de Proteção de dados o relatório de impacto é a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.[57]

Segundo o TSE e a ANPD, em seu Guia Orientativo - Aplicações da Lei Geral de Proteção de Dados por agentes de tratamento no contexto eleitoral, o relatório de impacto em relação ao tratamento de dados deverá ser elaborado principalmente em cenários de alto risco, como os que envolvam tratamento de dados sensíveis e em larga escala, é altamente recomendável.[58]

É recomendado pela ANPD que o relatório de impacto seja elaborado antes do início do tratamento de dados desejado pela empresa, isto para que seja possível analisar os impactos deste tratamento e entender se realmente vale a pena continuar com a operação. Sobre a publicidade do relatório o guia afirma:

> Embora a divulgação do RIPD não seja, em regra, obrigatória, permitir o acesso ao público em geral pode ser uma medida que demonstra a preocupação do controlador com a segurança dos dados pessoais que estão sob sua responsabilidade e seu compromisso com a privacidade dos titulares, além de atender aos princípios do livre acesso, da transparência e da responsabilização e prestação de contas.[59]

Portanto, é de extrema importância que em casos em que haja o tratamento de dados sensíveis, em grande escala ou que possam trazer algum grande risco aos titulares o relatório de impacto seja realizado, visando uma análise do cenário, bem como para entender se realmente vale dar continuidade ao processo idealizado.

---

[56] EM DIREÇÃO a um método para avaliações de impacto sobre a proteção de dados: entendendo as exigências do RGPD. 2019. - (-) - VRIJE UNIVERSITEIT BRUSSEL, [S. l.], -. Disponível em: https://cris.vub.be/ws/portalfiles/portal/51221989/dpialab_pb2019_1_final_PT.pdf. Acesso em: 24 out. 2023.

[57] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 13 set. 2023

[58] TRIBUNAL SUPERIOR ELEITORAL. -. GUIA ORIENTATIVO APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) por agentes de tratamento no contexto eleitoral, [S. l.], 24 out. 2023. Disponível em: https://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/guia-orientativo-aplicacao-da-lgpd.pdf. Acesso em: 24 out. 2023.

[59] RELATÓRIO de Impacto à Proteção de Dados Pessoais (RIPD). [S. l.], 24 out. 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd/relatorio-de-impacto-a-protecao-de-dados-pessoais/#p7. Acesso em: 24 out. 2023.

6.2 *Privacy by design*

De acordo com Bruno Bioni, o *Privacy by design* é a ideia em que se utiliza a proteção de dados como norteadora para a concepção de produtos e serviços que são desenvolvidos, devendo esses serem embarcados com tecnologias que facilitam o controle e proteção das informações pessoais dos seus usuários. Sendo assim uma boa prática com relação à proteção de dados e privacidade.[60]

O Privacy by design é norteado por alguns princípios, quais sejam, proativo, e não reativo; preventivo, e não corretivo, em que o intuito é prever e prevenir que incidentes de proteção de dados ocorram, antes que eles de fato possam ocorrer na prática. Isto impede que a empresa seja pega de surpresa e tenha que gastar mais investimento e esforços para remediar uma situação que poderia ter sido evitada, se analisada previamente pela equipe de segurança das informações e dados.[61]

O segundo princípio se trata do princípio da privacidade como padrão, *privacy by default,* por ele se entende que a privacidade deve ser automaticamente estabelecida como a configuração primária em todo sistema ou prática comercial, sem demandar qualquer intervenção ou ajuste do usuário. Isto é, o titular não necessita realizar qualquer ação para aceitar definições de confidencialidade mais rígidas; elas estão previamente integradas de forma convencional no produto, tecnologia ou serviço. Por conseguinte, a finalidade do processamento de informações deve ser precisa, transparente, restrita e pertinente às circunstâncias.

Outro princípio muito importante no *privacy by design* é a privacidade incorporada ao *design*, em que a privacidade representa um elemento fundamental do sistema, sem comprometer sua capacidade operacional. Ademais, o princípio da funcionalidade total, diz respeito à abordagem em que tem se o pensamento de somar e permitir que a funcionalidade total do sistema ou do projeto analisado traga benefícios e resultados a todos, reunindo todos os interesses e objetivos legítimos daquela organização e não apenas os que possuem relação com a privacidade, incorporando, por exemplo, a privacidade nas tecnologias utilizadas, nos processos e sistemas sem prejudicar a sua funcionalidade total.

---

[60] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. rev. atual. e aum. [S. l.: s. n.], 2020.

[61]PRIVACY by desing. [S. l.]. Disponível em: https://iapp.org/resources/article/sample-addendum-addressing-article-28-gdpr-and-incorporating-standard-contractual-clauses-for-controller-to-processor- transfers-of-personal-data/. Acesso em: 25 out. 2023.

Ademais, tem-se o princípio da segurança de ponta a ponta e proteção durante todo o ciclo de vida do dado, isto é, manter a confidencialidade, a integridade e a disponibilidade do dado durante todo o ciclo de sua vida.

Outrossim, tem-se o princípio da visibilidade e transparência, neste princípio, percebe-se que a privacidade assume o papel de trazer confiança aos titulares, através da transparência e visibilidade das condutas dos agentes de tratamento. Todos os termos e políticas ligados à confidencialidade necessitam ser registrados e transmitidos de maneira adequada, bem como devem ser atualizados periodicamente para que se adequem a realidade da empresa naquele momento. É importante ter em mente que a aquisição de informações pessoais implica a responsabilidade de salvaguardar os dados, sendo crucial implementar procedimentos de conformidade que possibilitem supervisionar, avaliar e assegurar a adesão às políticas de privacidade.

Por fim, pode se falar no princípio do respeito pela privacidade do usuário, em que procura-se manter os interesses dos titulares acima de tudo, fazendo com que as medidas adotadas pela empresa sejam arquitetadas em torno e em função dos interesses e necessidades dos seus titulares de dados pessoais.

6.3 Segurança no tratamento de dados

Além disso, é muito importante que as adequações feitas como boas práticas atinjam também as tecnologias utilizadas nos processos. Portanto, é de extrema relevância que a empresa analise se as plataformas e sistemas utilizados também auxiliam e agem no sentido de manter a privacidade e proteção dos dados dos usuários. Algumas boas práticas nesse sentido podem ser:

6.3.1 Controle de acessos

Controlar acessos é uma tarefa extremamente importante, isto, tendo em vista a necessidade de se manter os dados e informações sob o controle e a disposição do menor número de colaboradores possível, buscando evitar acessos indevidos, vazamentos inesperados, entre outros.

O controle de acessos vale tanto para plataformas, sistemas, pastas, arquivos físicos, armários, locais da empresa, setores, entradas, entre outros. Segundo Daniel Donda, existem alguns critérios para definir esses acessos, tais como:

> MACL (Mandatory Access Control List) – Mandatório: apenas o administrador pode definir quem pode acessar e qual o nível de acesso ao objeto.
> •DACL (Discretionary Access Control List) – Discricionário: método utilizado pelo Windows no qual o acesso ao objeto pode ser definido não somente pelo administrador, mas também pelo usuário, que, com uma certa permissão, terá a capacidade de conceder permissão a outros.
> RBAC (Role-Based Access Control): é o controle de acesso baseado em funções. Ao usar esse método, é possível criar funções e grupos para conceder o acesso apropriado ao objeto.[62]

É recomendável que a liberação de acessos aos colaboradores que trabalham operando dados e informações seja feita de forma estratégica e analisada. O gestor ou diretor deve analisar, no momento da liberação, se aquele colaborador de fato necessita daquele acesso que será concedido, se o acesso precisa de alguma restrição, se será um acesso temporário ou não, entre outros aspectos. Além desta análise, também é importante que o gestor revise os acessos concedidos periodicamente para entender se o colaborador já cumpriu a finalidade daquele acesso e pode ser retirado, se o colaborador mudou de função ou cargo dentro da empresa, entre outros.

6.3.2 Criptografia

A criptografia também é entendida como uma boa prática que pode auxiliar nos processos internos da empresa, considerada também como uma prática de *privacy by design*.[63]

De acordo com Daniel Donda, a criptografia funciona da seguinte forma:

> Criptografar o disco rígido é um controle de segurança importante, pois o usuário pode armazenar dados pessoais no disco e, em caso de perda, furto ou roubo, tudo o que estiver no disco estará protegido. É possível ativar a criptografia nativamente pelo bitlocker, uma ferramenta nativa da Microsoft disponível para Windows Vista, Windows 7, Windows 8 e Windows 10. Esse recurso irá proteger o sistema em caso de roubo em que o atacante pode tentar utilizar o disco rígido em alguma outra máquina para ler as informações.É possível também fazer uso da funcionalidade do bitlocker to go, que permite a criptografia de unidades de dados externas, como pen drives ou HDs externos. Para alguns computadores, é possível fazer uso do chip Trusted Platform Module (TPM), que é utilizado para armazenar as chaves de encriptação. Ativar a criptografia da unidade de disco é bem simples e isso pode ser feito em cada um dos computadores, porém é recomendado ativar por meio de políticas de grupo. É possível também criptografar arquivos individuais utilizando o sistema de criptografia Encrypting File System (EFS), que funciona no sistema de arquivos NTFS e

[62] DONDA, Daniel. Guia prático da implementação da LGPD. [S. l.]: Labrador, 2020.
[63] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. rev. atual. e aum. [S. l.: s. n.], 2020.

> não necessita de configuração para ser utilizado, porém é altamente recomendável criar uma política de recuperação de chaves de criptografia.[64]

6.3.3 Antivírus

Os antivírus são mais uma boa prática que possui o intuito de proteger os sistemas operacionais de vírus. O sistema utilizado pelas empresas corre o risco de ser comprometido quando ocorre a conexão de um dispositivo USB durante uma reunião, por exemplo, com o intuito de transferir arquivos, ao abrir e lançar anexos contidos em e-mails, ou ao visitar websites com conteúdo não verificável. A cada dia, são geradas inúmeras variações de programas maliciosos, sendo essas as principais causas de incidentes de segurança.

Por isso, é essencial manter um software antivírus em funcionamento e com as últimas atualizações disponíveis.Essa tarefa, na maior parte das empresas, fica com o time de TI ou segurança da informação.[65]

6.3.4 Política de senhas

A política de senhas possui a finalidade de estabelecer um padrão de criação e utilização de senhas fortes pelos colaboradores e parceiros da empresa, no intuito de evitar que pessoas mal intencionadas e *hackers* as descubram e se passem por pessoas autorizadas para a função, acessando, por exemplo, contas de *emails*, rede interna da empresa e sistemas, sites indevidos ou informações privilegiadas da organização como se fosse o proprietário daquele acesso.[66]

Algumas empresas utilizam os seguintes requisitos para a senha para que a mesma possa ser mais forte e, consequentemente, mais difícil de ser descoberta por terceiros alheios à organização: Tamanho de no mínimo 8 caracteres; contendo, no mínimo: uma letra maiúscula, uma letra minúscula, um número de 0 a 9 e um caractere especial, tais como : ! @ # $ % ^ & * - _ + = [ ] { } | \ : ‘, . ? / ` ~ “ < > ( ). Ademais, é bem interessante que esta senha seja modificada, com os mesmos requisitos em relação à nova senha, periodicamente, para fazer com que seja ainda mais complicado para o terceiro descobrir a senha utilizada por aquele colaborador.

---

[64] DONDA, Daniel. Guia prático da implementação da LGPD. [S. l.]: Labrador, 2020.
[65] DONDA, Daniel. Guia prático da implementação da LGPD. [S. l.]: Labrador, 2020.
[66] POLÍTICA DE SENHAS. [S. l.]. Disponível em: https://tic.fgv.br/sites/tic.fgv.br/files/arquivos/politica_de_senhas.pdf. Acesso em: 25 out. 2023.

6.3.5 Autenticação multifator

Segundo a Microsoft, a autenticação é o processo pelo qual o usuário passa para provar que é o próprio quem está utilizando determinado serviço. Normalmente esse processo é feito através de um login, composto por usuário e senha. Entretanto, tal método não é tão eficaz na prática, tendo em vista a praticidade de descobrir determinados logins por terceiros alheios à operação analisada.[67]

Por isso, muitas empresas e sistemas adotaram a autenticação multifator ou verificação em duas etapas, que é entendido como o processo que o usuário deve realizar ao acessar pela primeira vez um novo dispositivo ou aplicativo, em que o mesmo precisa mais do que acessar o seu usuário e senha, necessitando assim de um segundo fator para comprovação da sua identidade.

Os fatores mais utilizados nesses casos são senhas ou PINs, impressão digital, reconhecimento facial, uma mensagem via SMS, entre outros.

Daniel Faustino menciona a autenticação MFA, sendo esta caracteriza:

> A autenticação MFA oferece um mecanismo que garante acesso a um sistema por meio da validação de várias credenciais apresentadas pelo usuário. Estas credenciais geralmente estão ligada a três grupo de informação, quais sejam: conhecimento, possessão e presença física. Senhas e outras informações que possam ser memorizadas pelo usuário correspondem ao grupo de fatores de conhecimento. Dispositivos, tokens, cartões e outros elementos físicos que podem ser usados como mecanismos de autenticação são parte do grupo de fatores de possessão. Finalmente, o fator de presença física está relacionada a credenciais baseadas em informação biométrica como impressão digital, palma da mão, íris, face, perfil de voz e quaisquer outras características físicas que identifiquem um usuário unicamente. [68]

O autor ainda menciona em seu trabalho sobre autenticação biométrica, informando que tal mecanismo se utiliza de características próprias de cada indivíduo para identificá-lo de forma única naquele processo. Em um sistema de verificação, a informação biométrica do titular é comparada a um conjunto de informações previamente armazenadas em um banco de dados daquele usuário. Já no sistema de identificação, o dado biométrico é comparado a um

---

[67] O QUE é: Autenticação multifator. [S. l.]. Disponível em: https://support.microsoft.com/pt-br/topic/o-que-%C3%A9-autentica%C3%A7%C3%A3o-multifator-e5e39437-121c-be60-d123-eda06bddf661. Acesso em: 25 out. 2023.

[68] DE SOUZA, Daniel Faustino Lacerda. Um método para autenticação multifator baseado em biometria, interferência de onda e mapas caóticos. [S. l.: s. n.], 2017. Disponível em: https://repositorio.ufrn.br/bitstream/123456789/23949/1/DanielFaustinoLacerdaDeSouza_TESE.pdf. Acesso em: 25 out. 2023.

conjunto de informações em uma base de dados, a fim de identificar aquele usuário ao qual o dado pertence.

Mediante ao exposto, entende-se que não existem práticas obrigatórias para cada empresa em relação à segurança dos dados tratados, mas tanto o usuário quanto a sociedade espera que a empresa invista todo e qualquer esforço possível, bem como técnicas, inovações e tecnologias para garantir a maior segurança dos dados possível.

7 ESTUDO DE CASOS REAIS E ATUAÇÃO DA ANPD

A Lei Geral de Proteção de Dados foi publicada oficialmente no Diário Oficial no ano de 2018 e neste mesmo ano foi criada a Medida Provisória 869 que criava a ANPD - Autoridade Nacional de Proteção de Dados, sendo a sua estrutura criada apenas no ano 2020. A criação da ANPD se dá frente a necessidade de um órgão de fiscalização e monitoramento do cumprimento da Legislação de Proteção de Dados. E não somente a fiscalização, mas as sanções pelo descumprimento da LGPD entram em vigor no ano de 2021.[69]

Ademais, em 24 de fevereiro de 2023 surge a Resolução CD/ANPD nº 4 trazendo o regulamento de dosimetria e aplicação das sanções administrativas da LGPD[70], tendo como base os critérios do modelo de valoração, ponto central, atenuante e agravantes e os impactos causados aos titulares para definir a dosimetria das sanções.

É importante ressaltar que a LGPD desde sua criação traz em seu artigo 52 as sanções que podem ser aplicadas aos agentes de tratamento em casos em que os mesmos infrinjam alguma das normas previstas em seu texto legal, sendo essas sanções: advertência, com indicação de prazo para adoção de medidas corretivas; multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 por infração; multa diária; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 meses, prorrogável por igual período; proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.[71]

A Resolução nº 4, por outro lado, traz quando e como essas sanções serão aplicadas no caso concreto pela Autoridade Nacional de Proteção de Dados - ANPD, levando em consideração um regulação responsiva por parte da ANPD, isto é, antes de aplicar

---

[69] OBSERVATÓRIO LGPD. [S. l.]. Disponível em: https://www.observatorioprivacidade.com.br/. Acesso em: 19 out. 2023.

[70] PUBLICAÇÕES da ANPD. [S. l.], 28 maio 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em: 19 out. 2023.

[71] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 13 set. 2023

efetivamente a sanção prevista em Lei, a ANPD em seu exercício cotidiano e no caso concreto adotará incentivos em face dos agentes de tratamento, realizará atividades preventivas e orientativas e adotará a gradatividade da sanção em último caso, quando necessário, com relação à gravidade da situação relacionada à alguma transgressão da Lei.[72]

Alguns pontos muito importantes que serão levados em consideração no momento da dosimetria das sanções previstas na LGPD é a adoção de boas práticas pelos agentes de tratamento, sendo essas regras elaboradas pela própria organização para atender melhor às disposições da própria Lei, bem como a existência de um programa de governança e privacidade, sendo este uma estrutura de governança para demonstrar o comprometimento da organização com a Legislação.[73]

Outro critério utilizado para a dosimetria das sanções administrativas é a lógica da consequência e do risco auferidos na conduta do agente ou do incidente ocasionado. Além deste critério, a Resolução nº4 ainda criou uma ordem das sanções de acordo com a gravidade da infração, sendo a advertência a mais branda de todas e as suspensões e a proibição do tratamento de dados as mais graves.

Além da criticidade da sanção, a Resolução nº 4 ainda define uma escala de gravidade para as infrações, para que assim se possa analisar qual sanção deverá ser aplicada. Uma infração considerada média seria quando a situação impede ou limita o exercício de direitos ou a utilização de um serviço, assim como ocasiona danos materiais ou morais aos titulares, como por exemplo, a discriminação, fraudes financeiras, uso indevido de identidade, entre outros. Já a infração grave, se observa quando existe uma infração média adiciona a uma das seguintes hipóteses: a)Dados em larga escala; b) vantagem econômica decorrida da infração; c) dados sensíveis ou de criança, adolescente ou idoso;d) não enquadramento em uma das bases legais da LGPD; e) tratamento com efeitos discriminatórios, ilícitos ou abusivos; f) adoção sistemática de práticas irregulares; ou em casos em que a conduta caracteriza uma obstrução à fiscaliza.

---

[72] MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA/AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. RESOLUÇÃO CD/ANPD nº 04, de 24 de fevereiro de 2023. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. [S. l.], 24 fev. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 19 out. 2023.

[73] MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA/AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. RESOLUÇÃO CD/ANPD nº 04, de 24 de fevereiro de 2023. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. [S. l.], 24 fev. 2023. Disponível em:https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 19 out. 2023.

As infrações leves, por sua vez, são definidas como as excluídas das condutas que caracterizam infrações médias e infrações graves.[74]

Além da dosimetria, todas as sanções aplicadas devem partir de uma decisão fundamentada da Autoridade Nacional de Proteção de Dados, assegurando o direito à ampla defesa, ao contraditório e ao devido processo legal dos agentes de tratamento.

Para ilustrar o exposto, tem se, inicialmente, o caso do Facebook, condenado pela 29ª vara Civil de Belo Horizonte/MG pelo vazamento de dados ocorrido nos anos de 2018 e 2019 a título de danos morais coletivos e individuais. Segundo o processo de número 5127283-45.2019.8.13.0024, ocorreu o vazamento de dados de cerca de 29 milhões de pessoas através de hackers.

> A rede social pertencente a empresa Facebook Serviços Online do Brasil S/A foi alvo de um ataque, no qual hackers obtiveram acesso às contas de cerca de 29 milhões de pessoas, apropriando-se de detalhes de contato dos usuários, sendo que os hackers conseguiram acessar detalhes de contato, incluindo nome, número de telefone e e-mail de 15 milhões de pessoas, sendo que outras 14 milhões tiveram ainda mais dados acessados, como nome de usuário, gênero, localidade, idioma, status de relacionamento, religião, cidade natal, data de nascimento, dispositivos usados para acessar o Facebook, educação, trabalho e os últimos dez locais onde estiveram ou nos quais foram marcados e, não obstante, meses após o vazamento acima noticiado, um novo vazamento foi divulgado pela empresa de segurança virtual UpGuard, no dia 03 de abril de 2019 e, dessa vez, o vazamento atingiu dados mais sensíveis, expondo senhas de 22 mil contas e detalhes da movimentação de mais de 540 milhões de usuários, restando evidente o interesse comercial das informações vazadas, haja vista que os dados foram encontrados nos servidores de nuvem da empresa Amazon e continham informações de curtidas, comentários, imagens, entre outras interações na rede social.[75]

Na sentença, o juiz menciona a relação estreita entre o Código de Defesa do consumidor e a Lei Geral de Proteção de dados, buscando-se a defesa dos consumidores em relação aos seus dados pessoais vinculado à uma vulnerabilidade por parte destes. Foi constatada ainda a vulnerabilidade do sistema utilizado pela empresa devido a falha neste sistema, considerando se o risco da atividade exercida, não podendo ser alegado a culpa exclusiva de terceiros.

---

[74] MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA/AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. RESOLUÇÃO CD/ANPD nº 04, de 24 de fevereiro de 2023. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. [S. l.], 24 fev. 2023. Disponível em:https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 19 out. 2023.

[75] PODER JUDICIÁRIO DO ESTADO DE MINAS GERAIS - 29ª VARA CÍVEL DA COMARCA DE BELO HORIZONTE. SENTENÇA nº -, de 24 de julho de 2023. -. [S. l.]. Disponível em: https://www.migalhas.com.br/arquivos/2023/8/9F7CBE9C1EDBAE_5127283-45.2019.8.13.0024_9872.pdf. Acesso em: 19 out. 2023.

> Ora, tal circunstância demonstra a violação desarrazoada da segurança do serviço fornecido réu, descumprindo o artigo 6º, incisos I e III, do CDC e artigo 6º, inciso VII e VIII, da Lei n.º 13.709/2018. Cumpre registrar que a ocorrência de tal episódio era previsível em se tratando deste tipo de atividade e, mesmo diante da qualidade e de mecanismos de segurança que o réu deve oferecer, tal constatação não afasta a conclusão de que o sistema é vulnerável. E a falha desse sistema deve ser atribuída a quem dele usufrui como fonte de lucro. É o chamado risco da atividade, não havendo que se falar em culpa exclusiva de terceiro.[76]

Outro caso prático que ilustra o exposto é o caso do Instituto de Assistência ao Servidor Público Estadual de São Paulo – IAMSPE, que foi sancionado pela ANPD sendo lhe imposto duas advertências, acompanhadas de medidas corretivas.As sanções foram aplicadas devido ao comportamento impróprio do IAMSPE em relação a um incidente de segurança que envolveu informações pessoais, como CPF, nome, RG, endereço, número de telefone, salário, além de documentos, como CNH, RG e comprovante de residência de funcionários públicos do estado de São Paulo e seus familiares, que foram acessados sem autorização por um indivíduo externo.[77]

Uma das sanções aplicadas está relacionada à inobservância do artigo 48 da LGPD, que exige que o responsável pelos dados pessoais informe prontamente à ANPD e aos titulares sobre o incidente de segurança de dados pessoais. No referido caso, o Instituto demorou 3 meses após ter conhecimento do incidente para efetuar a notificação à ANPD. Além disso, o IAMSPE não cumpriu o prazo estipulado pela ANPD para comunicar individualmente os titulares de dados afetados pelo incidente. Quando o fez, faltaram informações essenciais, como uma descrição da natureza dos dados afetados, detalhes dos titulares envolvidos e justificativas para a demora na notificação. De acordo com a análise da gravidade do ocorrido, essa infração foi considerada séria, uma vez que envolvia informações pessoais de crianças, adolescentes e idosos.

A outra sanção diz respeito ao artigo 49 da LGPD, que estipula que os controladores devem utilizar sistemas que atendam aos requisitos de segurança, boas práticas, governança e princípios gerais estabelecidos na lei. No presente caso, o Instituto não estabeleceu controles

---

[76] PODER JUDICIÁRIO DO ESTADO DE MINAS GERAIS - 29ª VARA CÍVEL DA COMARCA DE BELO HORIZONTE. SENTENÇA nº -, de 24 de julho de 2023. -. [S. l.]. Disponível em: https://www.migalhas.com.br/arquivos/2023/8/9F7CBE9C1EDBAE_5127283-45.2019.8.13.0024_9872.pdf. Acesso em: 19 out. 2023.

[77] MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA/AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS/COORDENAÇÃO-GERAL DE FISCALIZAÇÃO. DESPACHO DECISÓRIO nº -, de 6 de outubro de 2023. Processo Administrativo Sancionador nº 00261.001969/2022-41. [S. l.], 6 out. 2023. Disponível em: https://www.in.gov.br/web/dou/-/despacho-decisorio-514655381. Acesso em: 20 out. 2023.

adequados para assegurar a confidencialidade dos dados pessoais armazenados no Portal do Beneficiário e não registrou informações (logs) no momento do incidente. No contexto desse incidente, o sistema continha uma grande quantidade de informações pessoais relacionadas a indivíduos vulneráveis, como crianças, adolescentes e idosos, e, por esse motivo, a infração também foi considerada grave. [78]

Portanto, através dos casos listados pode-se perceber tanto que os Tribunais de Justiça têm utilizado a Lei Geral de Proteção de Dados para fundamentar suas decisões, como também a Autoridade Nacional de Proteção de Dados têm adotado sanções administrativas para com as empresas que infringem alguma norma prevista na Legislação quanto a proteção de dados e segurança da informação.

[78] MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA/AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS/COORDENAÇÃO-GERAL DE FISCALIZAÇÃO. DESPACHO DECISÓRIO nº -, de 6 de outubro de 2023. Processo Administrativo Sancionador nº 00261.001969/2022-41. [S. l.], 6 out. 2023. Disponível em: https://www.in.gov.br/web/dou/-/despacho-decisorio-514655381. Acesso em: 20 out. 2023.

CONCLUSÃO

Portanto, mediante ao exposto no presente trabalho, pode se concluir que a Lei Geral de proteção de dados, assim como as demais Legislações pertinentes ao tema de proteção de dados, possui como um dos seus fundamentos a preocupação com a garantia dos direitos dos titulares de dados, bem como com a sua segurança e transparência em processos e operações cotidianas das empresas.

Entretanto, não há que se falar em uma restrição total no manuseio de dados por parte das empresas, pelo contrário, a própria Lei Geral de Proteção de Dados também traz como fundamento a livre iniciativa por parte das empresas, agentes de tratamento. Em nenhum momento a legislação voltada para proteção de dados e privacidade deseja privar que as empresas realizem suas atividades da forma que almejam, mas prevêem que as mesmas devem fazer isto com respeito à todas as garantias dadas aos titulares de dados, de forma transparente e segura.

Ademais, a permissão do tratamento de dados pelas empresas traz consigo a necessidade da observância de princípios e normas estipuladas em Lei. Conforme estudado, os agentes de tratamento se tornam responsáveis por suas atitudes, proporcionalmente ao seu poder de decisão na operação analisada, levando em consideração seus esforços para que incidentes possam ser evitados durante sua atividade.

Outro ponto de extrema relevância, é entender que o usuário, titular de dados, é a parte vulnerável da relação agente de tratamento - titular, tendo em vista que não possui completo domínio e ciência do que ocorre com seus dados dentro dos bancos de dados das empresas. Em face desta problemática, a Lei Geral de proteção de dados enumera diversos direitos aos titulares, que podem ser exigidos a qualquer momento, através de um canal de solicitação que deverá ser disponibilizado pela empresa.

Além dos direitos dos titulares, a Lei ainda traz a utilização de bases legais de tratamento de dados, sendo essas hipóteses taxativas de quando o agente de tratamento poderá exercer o tratamento de dados, fora delas, não se é permitido a utilização desses dados coletados.

Além disso, o trabalho aborda o meio virtual como cenário de pesquisa, ficando comprovado que o mesmo traz diversos obstáculos, bem como soluções para o tratamento de dados em massa. Isto tendo em vista que o compartilhamento de informações pelo meio digital é muito mais rápido e possui um alcance muito maior, mas ao mesmo tempo também

permite que o tratamento se torne cada vez mais seguro, tendo em vista as tecnologias de controle de acesso, tais como senhas, logins, criptografia, entre outros.

O processo interno do tratamento de dados também é muito relevante para a resolução da incógnita levantada no presente trabalho, tendo em vista, que o mesmo deverá ser norteado pela transparência e segurança das operações. Uma empresa bem estruturada e com uma gestão antenada à proteção de dados irá disponibilizar um bom programa de governança, além de adotar boas práticas neste sentido.

Isto permite que o titular de dados possa compreender como os seus dados são tratados de forma documentada através de mapeamento de dados, políticas, termos e treinamento dos colaboradores internos da empresa. Permitindo, assim, que o titular tenha um certo controle do quê será feito com suas informações, além da transparência por parte da empresa.

Por fim, pode se entender que a ANPD, assim como os Tribunais, já possuem decisões em que as empresas devem se responsabilizar pelo tratamento indevido dos dados, seja porque não utilizaram uma base legal devida, não possuem documentações suficientes, entre outros fatores, demonstrando a real imposição das normas no tocante a proteção de dados.

REFERÊNCIAS

BIONI, Bruno; DIAS, Daniel. RESPONSABILIDADE CIVIL NA LGPD: construção do regime por meio de interações com o CDC. In: Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: BR Bioni Sociedade Individual de Advocacia, p. 394-495, 2021.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. rev. atual. e aum. [*S. l.*: *s. n.*], 2020.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidente da República, [2016]

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

CONTRACT. [S. l.], 18 out. 2023. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/contract/. Acesso em: 18 out. 2023.

COTS, Márcio; OLIVEIRA, Ricardo. Lei geral de proteção de dados pessoais comentada. 4. ed. rev. atual. e aum. [*S. l.*: *s. n.*], 2020.

DE SOUZA, Daniel Faustino Lacerda. Um método para autenticação multifator baseado em biometria, interferência de onda e mapas caóticos. [S. l.: s. n.], 2017. Disponível em: https://repositorio.ufrn.br/bitstream/123456789/23949/1/DanielFaustinoLacerdaDeSouza_TESE.pdf. Acesso em: 25 out. 2023.

DONDA, Daniel. Guia prático da implementação da LGPD. [S. l.]: Labrador, 2020.

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

EM DIREÇÃO a um método para avaliações de impacto sobre a proteção de dados: entendendo as exigências do RGPD. 2019. - (-) - VRIJE UNIVERSITEIT BRUSSEL, [S. l.], -. Disponível em: https://cris.vub.be/ws/portalfiles/portal/51221989/dpialab_pb2019_1_final_PT.pdf. Acesso em: 24 out. 2023.

ENTENDA o conceito de Privacy by Design e sua relação com a LGPD. [S. l.], 25 out. 2023. Disponível em: https://getprivacy.com.br/privacy-by-design-lgpd/. Acesso em: 25 out. 2023.

GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

GONÇALVES, Vitor Hugo Pereira. Marco Civil da Internet Comentado. São Paulo: Atlas, 2017.

GUIA Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. 2. ed. [S. l.: s. n.], 2022. Disponível em: https://drive.google.com/file/d/1lGflXGOXambguB6T8ieEbHC9qNOLvTKR/view. Acesso em: 20 out. 2023.

ISO 27001: Curso completo para certificação EXIN ISFS!. [S. l.], 24 out. 2023. Disponível em: https://www.udemy.com/course/isfs-iso27001/. Acesso em: 24 out. 2023.

MAGALHÃES, Guilherme. Contratos eletrônicos de consumo. 3. ed. rev. atual. e aum. [*S. l.*: *s. n.*], 2016.

MARTINS, Guilherme Magalhães. Direito Privado e Internet. São Paulo: Atlas, 2014.

MASSON, Nathalia. Manual de Direito Constitucional. 4ª. ed. rev. atual. e aum. [*S. l.*]: Juspodivm, 2016.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA/AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS/COORDENAÇÃO-GERAL DE FISCALIZAÇÃO. DESPACHO DECISÓRIO nº -, de 6 de outubro de 2023. Processo Administrativo Sancionador nº 00261.001969/2022-41. [S. l.], 6 out. 2023. Disponível em: https://www.in.gov.br/web/dou/-/despacho-decisorio-514655381. Acesso em: 20 out. 2023.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA/AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. RESOLUÇÃO CD/ANPD nº 04, de 24 de fevereiro de 2023. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. [S. l.], 24 fev. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 19 out. 2023.

MODULAÇÕES ALGORÍTMICAS: uma análise das tecnologias de orientação de comportamento a partir das patentes do Facebook. 2019. Dissertação apresentada ao Programa de Pós Graduação em Ciências Humanas e Sociais da Universidade Federal do ABC (UFABC) (Ciências Humanas e Sociais) [S. l.], 2019. Disponível em: file:///C:/Users/damar/Downloads/MODULACOESALGORITMICAS_dissertacaoDeboraMachado.pdf. Acesso em: 16 out. 2023.

OBSERVATÓRIO LGPD. [S. l.]. Disponível em: https://www.observatorioprivacidade.com.br/. Acesso em: 19 out. 2023.

PINHEIRO, Patrícia Peck. Direito Digital. 4. ed. rev. atual. e aum. [*S. l.*: *s. n.*], 2010.

PODER JUDICIÁRIO DO ESTADO DE MINAS GERAIS - 29ª VARA CÍVEL DA COMARCA DE BELO HORIZONTE. SENTENÇA nº -, de 24 de julho de 2023. -. [S. l.]. Disponível em: https://www.migalhas.com.br/arquivos/2023/8/9F7CBE9C1EDBAE_5127283-45.2019.8.13.0024_9872.pdf. Acesso em: 19 out. 2023.

POLÍTICA DE SENHAS. [S. l.]. Disponível em: https://tic.fgv.br/sites/tic.fgv.br/files/arquivos/politica_de_senhas.pdf. Acesso em: 25 out. 2023.

PRIVACY by desing. [S. l.]. Disponível em: https://iapp.org/resources/article/sample-addendum-addressing-article-28-gdpr-and-incorporating-standard-contractual-clauses-for-controller-to-processor-transfers-of-personal-data/. Acesso em: 25 out. 2023.

PUBLICAÇÕES da ANPD. [S. l.], 28 maio 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em: 19 out. 2023.

RELATÓRIO de Impacto à Proteção de Dados Pessoais (RIPD). [S. l.], 24 out. 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd/relatorio-de-impacto-a-protecao-de-dados-pessoais/#p7. Acesso em: 24 out. 2023.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Curso de Direito Constitucional. [*S. l.*: *s. n.*], 2017.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Responsabilidade e ressarcimento de danos por violação às regras previstas na LGPD: um cotejamento com o CDC. In: LIMA, Cíntia Rosa Pereira de (Coord.). Comentários à Lei Geral de Proteção de Dados. São Paulo: Almedina, 2020, p. 322.

TRIBUNAL SUPERIOR ELEITORAL. -. GUIA ORIENTATIVO APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) por agentes de tratamento no contexto eleitoral, [S. l.], 24 out. 2023. Disponível em: https://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/guia-orientativo-aplicacao-da-lgpd.pdf. Acesso em: 24 out. 2023.