Universidade Estadual de Londrina

BRENDA CAROLINA VICENTINI MUGNOL

OPERADOR:
ATUAÇÃO PARA ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS PESSOAIS COMO MEDIDAS DE SEGURANÇA

Londrina
2024

BRENDA CAROLINA VICENTINI MUGNOL

OPERADOR:
ATUAÇÃO PARA ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS PESSOAIS COMO MEDIDAS DE SEGURANÇA

Dissertação apresentada ao Programa de Pós-graduação em Direito Negocial da Universidade Estadual de Londrina - UEL, como requisito parcial para a obtenção do título de Mestre.

Orientador: Prof. Dr. Tarciso Teixeira

Londrina
2024

Ficha Catalográfica

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UEL

MUGNOL, BRENDA CAROLINA VICENTINI.
OPERADOR: ATUAÇÃO PARA ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS PESSOAIS COMO MEDIDAS DE SEGURANÇA / BRENDA CAROLINA VICENTINI MUGNOL. - Londrina, 2024.
85 f. : il.

Orientador: TARCISIO TEIXEIRA.
Dissertação (Mestrado em Direito Negocial) - Universidade Estadual de Londrina, Centro de Estudos Sociais Aplicados, Programa de Pós-Graduação em Direito Negocial, 2024.
Inclui bibliografia.

1. PRIVACIDADE; OPERADOR DE DADOS; ANONIMIZAÇÃO; PSEUDONIMIZAÇÃO - Tese. I. TEIXEIRA, TARCISIO. II. Universidade Estadual de Londrina. Centro de Estudos Sociais Aplicados. Programa de Pós-Graduação em Direito Negocial. III. Título.

CDU 34

BRENDA CAROLINA VICENTINI MUGNOL

OPERADOR:
ATUAÇÃO PARA ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS PESSOAIS COMO MEDIDAS DE SEGURANÇA DE DADOS COMO MEDIDAS DE SEGURANÇA

Dissertação apresentada ao Programa de Pós-graduação em Direito Negocial da Universidade Estadual de Londrina - UEL, como requisito parcial para a obtenção do título de Mestre.

BANCA EXAMINADORA

Prof. Orientador: Prof. Dr. Tarciso Teixeira
Universidade Estadual de Londrina - UEL

Profa. Dra. Renata Capriolli Zocatelli Queiroz
Faculdades Londrina - FL

Profa. Dra. Patricia Eliane da Rosa Sardeto
Pontifícia Universidade Católica - PUC

Londrina, 07 de novembro de 2024.

Dedico este trabalho a meus pais, que sempre me ensinaram o caminho da educação e sempre foram minha base. Dedico também ao meu marido, pelo apoio incondicional.

AGRADECIMENTOS

Ao meu orientador, professor Tarcisio, que trouxe todo o ensinamento que eu precisava para não só cursar e concluir o Mestrado, mas também conhecimentos que serão utilizados na docência e na vida. Agradeço a paciência em orientar, e por toda a ajuda neste trajeto.

A Deus, por ser meu sustento desde o início, me dando força e coragem para levantar e “batalhar” todos os dias, em busca de uma formação melhor, um futuro melhor, uma vida melhor, e a ser melhor como profissional e pessoa.

Aos meus pais, Eva Elizete Feliciano dos Santos Mugnol e Valdinei Sabatowisch Mugnol, que sempre me ensinaram o caminho correto a seguir. O caminho do ensino, de Deus, da humildade, de querer ser sempre uma pessoa melhor, e me deram todo o suporte para eu alcançar meus objetivos. Sem vocês eu nada seria.

Ao meu marido, Danilo Henrique Vicentini da Cruz, por ser meu alicerce, me incentivando a quebrar objeções, superar medos e a querer voar cada dia mais. Você tem grande participação durante esse mestrado.

Ao Omar Zebian, pelo apoio e incentivo tanto profissionalmente quanto para que eu seguisse meus sonhos na carreira acadêmica. Aos amigos de mestrado João Vitor e Desirée, pela parceria incondicional no decorrer de todo o curso, bem como, aos amigos da vida por compreenderem as ausências e renúncias que precisaram ser feitas e por me apoiarem e incentivarem sempre.

Aos professores, pelas lições trazidas, que contribuíram em muito, não somente com esta pesquisa, mas com a minha formação em sua totalidade.

A todos, meu muito obrigado.

"É justo que muito custe o que muito vale"

(Santa Teresa d'Ávila)

RESUMO

MUGNOL, Brenda Carolina. **OPERADOR:** ATUAÇÃO PARA ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS PESSOAIS COMO MEDIDAS DE SEGURANÇA. 2024. 85 páginas. Dissertação (Mestrado em Direito Negocial) – Centro de Estudos Sociais Aplicados, Universidade Estadual de Londrina, Londrina, 2024.

A proteção de dados pessoais tem se consolidado como um tema de extrema relevância, especialmente diante do aumento de incidentes de segurança envolvendo os vazamentos de informações. As normativas que regulam essa proteção evoluíram significativamente ao longo dos anos, com destaque para a atuação dos agentes de tratamento de dados, particularmente do operador de dados pessoais, que desempenha um papel central nos processos de proteção e mitigação de riscos associados à segurança. Este estudo enfoca o uso de técnicas de anonimização e pseudonimização como ferramentas que podem ser utilizadas como medidas de segurança para proteger dados sensíveis e minimizar os impactos negativos em caso de incidentes. Ambas as técnicas são essenciais para garantir a privacidade dos titulares, especialmente em contextos de tratamento de dados com finalidades específicas, como pesquisas acadêmicas, estudos sociais e bases de dados relacionadas à saúde pública. Para entender o papel do operador de dados nesses processos, foi realizada uma pesquisa bibliográfica, explorando a legislação vigente, posicionamentos doutrinários sobre o tema, definições relativas à tecnologia da informação e as melhores práticas de segurança de dados. A análise identificou que a anonimização, ao tornar os dados irreversivelmente não identificáveis, e a pseudonimização, ao permitir que identificadores sejam mantidos separados e seguros, não são apenas ferramentas cruciais para proteção, mas também estratégias para mitigar danos em situações de vazamento. O estudo concluiu que o operador de dados, em conjunto com o controlador, possui responsabilidades específicas na implementação e manutenção dessas técnicas. Ele deve garantir conformidade com os parâmetros legais e a aplicação de práticas adequadas de segurança para proteger os titulares. Por fim, a pesquisa reforça que a adoção de processos de anonimização e pseudonimização não apenas cumpre requisitos legais, mas também representa uma abordagem proativa para reduzir riscos de segurança, apesar de, por vezes, possuir custos elevados. Em síntese, a pseudonimização e a anonimização não garantem uma proteção absoluta, mas representam pilares fundamentais na construção de um ambiente digital mais seguro. A análise sistemática e contínua desses métodos contribui para um ambiente de maior confiança e proteção no tratamento de dados pessoais, especialmente em um cenário tecnológico e regulatório em constante evolução.

Palavras-chave: Privacidade; Operador de dados; Proteção de dados; Anonimização; Pseudonimização.

ABSTRACT

MUGNOL, Brenda Carolina. **OPERATOR:** ACTION FOR ANONYMIZATION AND PSEUDONYMIZATION OF PERSONAL DATA AS SECURITY MEASURES. 2024. 85 pages. Dissertação (Mestrado em Direito Negocial) – Centro de Estudos Sociais Aplicados, Universidade Estadual de Londrina, Londrina, 2024.

The protection of personal data has become an extremely important issue, especially given the increase in security incidents involving information leaks. The regulations governing this protection have evolved significantly over the years, with emphasis on the role of data processing agents, particularly the personal data operator, who plays a central role in the processes of protection and mitigation of risks associated with security. This study focuses on the use of anonymization and pseudonymization techniques as tools that can be used as security measures to protect sensitive data and minimize negative impacts in the event of incidents. Both techniques are essential for guaranteeing the privacy of data subjects, especially in contexts where data is processed for specific purposes, such as academic research, social studies and databases related to public health. In order to understand the role of the data operator in these processes, a bibliographical survey was carried out, exploring current legislation, doctrinal positions on the subject, definitions relating to information technology and best data security practices. The analysis identified that anonymization, by making data irreversibly unidentifiable, and pseudonymization, by allowing identifiers to be kept separate and secure, are not only crucial tools for protection, but also strategies for mitigating damage in leakage situations. The study concluded that the data operator, together with the controller, has specific responsibilities in implementing and maintaining these techniques. They must ensure compliance with legal parameters and the application of appropriate security practices to protect data subjects. Finally, the research reinforces that the adoption of anonymization and pseudonymization processes not only complies with legal requirements, but also represents a proactive approach to reducing security risks, despite their sometimes high costs. In short, pseudonymization and anonymization do not guarantee absolute protection, but they are fundamental pillars in building a safer digital environment. The systematic and continuous analysis of these methods contributes to an environment of greater trust and protection in the processing of personal data, especially in a constantly evolving technological and regulatory landscape.

Key-words: Privacy; Data operator; Data protection; Anonymization; Pseudonymization.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

Art.	Artigo
ANPD	Autoridade Nacional de Proteção de Dados
BC	Banco Central
CDC	Código de Defesa do Consumidor
CPC	Código de Processo Civil
CPF	Cadastro de Pessoas Físicas
DPO	Data Protection Officer
ENEM	Exame Nacional do Ensino Médio
GDPR	*General Data Protection Regulation*
LGPD	Lei Geral de Proteção de Dados Pessoais
MOAB	*Mother of All Breaches*
RRA	Risco de Reidentificação Aceitável
RRM	Risco de Reidentificação Mensurável
UE	União Europeia

SUMÁRIO

1 INTRODUÇÃO

O direito é uma integração normativa entre fatos segundo valores, sendo entendido a partir da teoria tridimensional estabelecida por Miguel Reale[1]. Desta teoria, compreende-se que a norma só ocorre em virtude de um fato, ou seja, os fatos e valores acabam por se tornar normas. Assim dá-se a compreensão de como ocorrem as evoluções legislativas, sendo o direito atuante em todas as inovações surgidas na sociedade e vindo sempre após as transformações para regulamentá-las.

Com enfoque nas mudanças ocorridas ao longo dos tempos, destacam-se as evoluções tecnológicas, das quais surgiram inúmeras inovações para o dia a dia da população em geral, por meio de mecanismos como *big data*, *blockchain*, inteligência artificial, entre outros.

As novas revoluções tecnológicas são baseadas principalmente na revolução digital e vêm mudando as nossas formas de interpretar o mundo e de se relacionar com ele, ao mesmo tempo em que exigem uma maior integração entre sociedade e tecnologia, vivenciando uma notável sociedade em redes.

A partir disto, o direito negocial é amplamente impactado por tais novas tecnologias, tendo em vista que as novas relações tendem a ser realizadas através do digital. Com o estabelecimento de relações jurídicas totalmente no meio digital se faz necessária uma intervenção legal mediante leis, jurisprudências e doutrinas a fim de regulamentar essas novas relações e proteger os indivíduos que as compõe.

Um grande marco advindo de tais evoluções foi a criação da Lei Geral de Proteção de Dados Pessoais (LGPD), que alterou o Marco Civil da Internet. Tal alteração sobreveio, entre outros motivos, com o fim de proteger principalmente os dados dos sujeitos nas relações estabelecidas por meio da internet, tornando-se a proteção de dados um direito constitucionalmente protegido dada a sua importância.

O dado, como informação, tornou-se um dos bens mais valiosos da atualidade. Empresas têm investido cada vez mais na aquisição de dados dos seus clientes e/ou usuários a fim de traçar estratégias de marketing e consumeristas, servindo a LGPD para regulamentar esse tratamento, coleta e compartilhamento dos

[1] REALE, Miguel. **Teoria Tridimensional do Direito**. 5 ed. rev. e aum. São Paulo: Saraiva,1994

dados.

Assim, a proteção de dados pessoais tornou-se um tema de grande relevância no cenário jurídico e tecnológico atual, impulsionada pelo crescimento exponencial do uso de informações em ambientes digitais. Com o advento de legislações como a Lei Geral de Proteção de Dados (LGPD), o tratamento de dados ganhou regras específicas, incluindo a definição de agentes de tratamento: o controlador, responsável por decidir sobre o tratamento, e o operador, que realiza o tratamento em nome do controlador. Em algumas situações, no entanto, uma empresa pode operar como controlador e operador ao mesmo tempo, sem distinguir essas funções.

Ainda, destaca-se que, quando do tratamento dos dados pessoais, existem processos relacionados ao mesmo que podem ser realizados pelo operador e pelo controlador. Entre tais processos encontram-se a anonimização e pseudonimização, os quais por sua vez servem para tornar dados anônimos, sendo o primeiro um processo que remove completamente os identificadores do dado, enquanto no segundo são substituídos por pseudônimos que tornem o dado não identificado.

A anonimização transforma os dados em informações que não permitem a identificação do titular, retirando seu caráter pessoal e, com isso, excluindo-os da proteção da LGPD. Já a pseudonimização substitui identificadores por pseudônimos, tornando os dados não identificáveis de imediato, mas ainda passíveis de reversão. Esses processos têm se mostrado de grande relevância como medidas de segurança, especialmente quando se fala sobre minimizar os impactos de vazamentos ou incidentes de segurança.

Diante deste cenário, o estudo se iniciará pela análise da legislação vinculada ao tema proteção de dados, com sua evolução histórica e as bases para o surgimento e delimitações da LGPD. Além da LGPD, serão analisadas as demais normas de proteção de dados em vigência no Brasil, tendo em vista que a LGPD sofreu grande influência do GDPR, legislação de proteção de dados da Europa, de forma que é possível também analisar as suas semelhanças e diferenças.

Construída a base para os tópicos subsequentes, o trabalho se aprofundará nos agentes de tratamento de dados brasileiros, os quais se dividem em

controlador e operador de dados pessoais, com a apresentação de cada um dentro de sua disciplina jurídica, debatendo ainda sobre sua atuação no tratamento de dados pessoais.

Quando se fala em tratamento de dados, também se faz necessário debater acerca dos incidentes de segurança, já que podem ocorrer, entre outros motivos, devido a falhas no tratamento realizado pelos agentes de tratamento. Assim, o trabalho abordará alguns dos vazamentos ocorridos no país com grande volume de dados vazados, a fim de identificar que tipos de dados foram vazados.

Assim, como sequência, serão apresentados os processos de anonimização e pseudonimização, com descrições sobre suas definições, seus trâmites legais e em que momento são utilizados, destacando a sua utilização como medida de segurança no tratamento dos dados pessoais de forma a diminuir os impactos negativos em casos de ocorrência de incidentes de segurança.

A implementação dessas técnicas traz desafios, incluindo custos financeiros e operacionais que podem ser um obstáculo, principalmente para pequenas e médias empresas. Ainda assim, quando adequadamente aplicados, esses processos podem reduzir significativamente os danos associados a incidentes, protegendo não apenas os titulares dos dados, mas também a reputação e a conformidade legal das empresas envolvidas.

Este estudo busca explorar especificamente o papel do operador de dados na execução desses processos, analisando como sua atuação pode influenciar a mitigação de riscos e o fortalecimento da segurança no tratamento de dados. O objetivo é compreender como o operador pode, por meio dessas práticas, agir como um elemento-chave na proteção dos dados pessoais e no cumprimento das exigências legais.

Ao final, o estudo apresentará suas conclusões, respondendo à questão de como o operador de dados usa a anonimização e a pseudonimização na atividade de tratamento como medida de segurança, não somente quando se trata de dados de pesquisas e dados de saúde, mas de forma geral, e que, apesar das dificuldades e desafios (a exemplo da questão financeira), podem ser importantes aliados na proteção de dados.

2 PROTEÇÃO DE DADOS: LEGISLAÇÃO PERTINENTE

A proteção de dados tem se mostrado cada vez mais relevante nos debates, sejam eles acadêmicos ou não. De acordo com Renata Capriolli Zocatelli Queiroz[2], a proteção do direito à privacidade é relevante devido às informações obtidas por aplicativos, tais como as informações de geolocalização, a análise do comportamento em rede dos usuários, o tempo de navegação em sites eletrônicos, dentre outras.

De acordo com a autora e Tarcisio Teixeira, existem muitos sites, jogos e serviços que parecem gratuitos, mas, na verdade, são cobrados por coletar informações dos usuários. Isso torna necessário uma lei específica sobre o assunto.

Segundo Bruno Bioni[3], "a tutela jurídica dos dados pessoais é um imperativo que impõe uma nova fronteira aos direitos da personalidade, a fim de que o fluxo informacional não seja corrosivo à esfera relacional da pessoa humana e, por tabela, ao livre desenvolvimento de sua personalidade".

A amplitude e a efetividade das garantias asseguradas à privacidade, como momentos constitutivos da esfera pública e da esfera privada, dependem, em grande parte, da possibilidade de que a sociedade da informação evolua para uma sociedade "do conhecimento e do saber" e não para uma sociedade da vigilância, da classificação e do controle, conforme afirma Stefano Rodotá[4].

Assim, ressalta-se que o assunto não surgiu atualmente, se tratando de uma grande evolução legislativa no decorrer do tempo, merecendo destaque tais evoluções a fim de compreender como a LGPD brasileira foi embasada.

2.1 Breve Histórico

Ao longo dos anos, surgiram diversos instrumentos que relacionavam a proteção de dados pessoais ao direito à privacidade, como a Lei de Hessen de 1970,

---

[2] QUEIROZ, Renata Capriolli Zocatelli. **A proteção de dados pessoais**: a LGPD e a disciplina jurídica do encarregado de proteção de dados pessoais. 2021. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2021. Disponível em: https://doi.org/10.11606/T.2.2021.tde-23082022-085834.

[3] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020

[4] RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

a Lei de Dados Suecos de 1973, o Estatuto Alemão de Proteção de Dados de Rheinland-Pfalz de 1974, e a Lei Federal de Proteção de Dados Alemã de 1977[5].

Portugal estabeleceu a autodeterminação informativa entre os seus direitos fundamentais, sendo o primeiro país a fazer isso, no ano de 1976, seguido pela Alemanha em 1983[6].

Em 2000, a Carta dos Direitos Fundamentais da União Europeia[7] definiu, em seu art. 8º, que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito". Além disso, tais dados "devem ser objeto de um tratamento leal, para fins específicos e com consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei", sendo certo que "todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação". Por fim, o cumprimento dessas regras "fica sujeito à fiscalização por parte de uma autoridade independente".

Na seara brasileira, a Lei 12.414, de 9 de junho de 2011, que trata do cadastro positivo, ampliou o alcance das normas atinentes aos bancos de dados e aos cadastros de consumidores, incluindo entre os direitos dos cadastrados o direito a obter o cancelamento do cadastro quando solicitado (art. 5º, I); o direito a conhecer os principais elementos e critérios considerados para a análise de risco (art. 5º, IV); o direito a ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento (art. 5º, V); o direito de solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados (art. 5º, VI), e o direito a ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados (art. 5º, VII)[8].

Em meio a tal legislação, em 2009 surgiu o primeiro projeto de regulamentação envolvendo a internet, o qual tramitou até 2011, tendo sido sancionado no ano de 2014. Desta regulamentação se originou a Lei nº 12.965 de 23 de abril de 2014, denominada de Marco Civil da Internet, a qual estabelece princípios,

---

[5] CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**, v. 13, p. 59-67, 2017.
[6] Op. Cit.
[7] EUROPARL. **CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA**. 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf
[8] BRASIL. **LEI Nº 12.414, DE 9 DE JUNHO DE 2011**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm.

garantias, direitos e deveres para o uso da internet no Brasil, bem como determina diretrizes para a atuação da União, dos Estados, Distrito Federal e Municípios em questões relacionadas à matéria.

O Marco Civil da Internet apresentou princípios norteadores do uso da internet no país, determinando que tem como base a liberdade de expressão, a livre iniciativa, a livre concorrência, a defesa do consumidor, entre outros[9].

Conferiu ainda proteção a direitos inerentes ao acesso à internet, previstos em seu artigo 7º, a exemplo da inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação. Também determinou ser inviolável e sigiloso o fluxo de suas comunicações pela internet, e as comunicações privadas armazenadas, salvo por ordem judicial, na forma da lei.

Ainda, há previsão expressa com relação a não suspensão da conexão com a internet, salvo por débito decorrente de sua utilização e manutenção da qualidade contratada da conexão a internet, assegurando assim o acesso à internet e sua continuidade para os usuários que se encontrarem em dia com os pagamentos.

Com relação à contratação do serviço, o Marco Civil da internet também trouxe regulamentação. O artigo 7º também estabelece, no inciso V, que as informações devem ser claras e completas nos contratos de prestação de serviços, com detalhamento sobre o regime de proteção dos registros de conexão e acesso a aplicações de internet, bem como, sobre práticas de gerenciamento da rede que possam prejudicar sua qualidade.

Deverão ser claras e completas as informações acerca da coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, conforme inciso seguinte, elencando para quais finalidades tais dados poderão ser utilizados. Com relação às finalidades, estas devem justificar sua coleta, não ser vedadas pela legislação e estar especificadas nos contratos de prestação de serviços ou termos de uso de aplicações de internet.

As políticas de uso dos provedores de conexão à internet e de aplicações da internet deverão ter publicidade e clareza, além de acessibilidade,

---

[9] BRASIL. **LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei.

Os dados coletados em decorrência dos serviços de internet não podem ser fornecidos a terceiros, inclusive se tratando de registros de conexão e de acesso a aplicações de internet, com a exceção de quando houver consentimento livre, expresso e informado (além das hipóteses previstas em lei).

O consentimento também precisa ser expresso, conforme o Marco Civil, sobre a coleta, uso, armazenamento e tratamento dos dados pessoais, os quais precisam ocorrer na forma destacada nas demais cláusulas contratuais.

Nas palavras de Tarcisio Teixeira:

> Sem dúvida, a norma teria feito melhor se, em vez de prever apenas consentimento expresso, tivesse disposto consentimento prévio e expresso. Com isso, alguns agentes econômicos poderão se utilizar de ferramentas para obter o consentimento posteriormente, de forma a dificultar a opção do usuário, que muitas vezes já estará envolvido com a ferramenta tecnológica que lhe foi oferecida e já está sendo utilizada[10].

Havendo requerimento, ao término da relação entre as partes, pelo titular do dado pessoal, deverá ocorrer a exclusão definitiva dos dados que houver fornecido a determinada aplicação de internet, ressalvadas as hipóteses de guarda obrigatória previstas em lei.

Aplicam-se também ao Marco Civil da Internet as normas de proteção de defesa do consumidor nas relações de consumo realizadas na internet. Nota-se que existem dispositivos do Marco Civil da internet que sofreram alterações pela Lei 13.709 de 2018, intitulada de Lei Geral de Proteção de Dados Pessoais (LGPD), diferenciando-se ambas as leis pelo fato de a LGPD abranger não somente o tratamento de dados no âmbito digital, mas fora da internet também.

Neste sentido, com relação às normas de defesa do consumidor, é importante ressaltar que tal legislação também possui regramentos atinentes à proteção de dados, desde antes da entrada em vigor da LGPD. As relações jurídicas mantidas entre um sujeito que realiza atividades de tratamento de dados e o titular desses dados, em regra, enquadram-se no conceito de relação de consumo

[10] TEIXEIRA, Tarcisio. **Curso de Direito e Processo Eletrônico: doutrina, jurisprudência e prática**. 4. ed. São Paulo: Saraiva, 2018

submetida ao microssistema do Código de Defesa do Consumidor.

As normas de proteção de dados previstas no Código de Defesa do Consumidor podem ser encontradas em vários artigos. Podemos citar acerca da necessidade de se fornecer informação adequada e clara sobre os serviços, com previsão no art. 6º, III do CDC, uma vez que a informação é relevante para conduzir a tomada de decisões, razão pela qual o seu controle e as regras de acesso têm relevância jurídica. Deste modo, na prestação de serviços de tratamento de dados pessoais, o consumidor deve ter devidamente informado sobre tudo o que será feito com os seus dados, o que compreende não somente a autorização, mas também o conhecimento, a retificação, a boa-fé, a interrupção e a exclusão de tais dados.

Outro ponto em que há previsão com relação ao tratamento de dados ainda no CDC, o consumidor titular de dados tem o direito de ser informado sempre que houver a inclusão de seus dados pessoais em cadastros, fichas, registros ou banco de dados, quando tiver sido aberto sem o seu consentimento, com previsão no art. 43, *caput* e § 2º, do CDC. No parágrafo terceiro do mesmo artigo, fica claro que o consumidor poderá exigir imediatamente correção de seus dados.

Ainda, importa destacar o fato de a proteção de dados ter se tornado direito constitucional, advindo da EC 115 de 10 de fevereiro de 2022, a qual alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Dentre os dispositivos alterados, incluiu-se o inciso LXXIX no artigo 5º, informando ser assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Antes mesmo disto, e após a LGPD, surgiu ainda a Medida Provisória nº 869, de 27 de dezembro de 2018, a qual veio para alterar a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados (ANPD). Tal medida provisória foi convertida na Lei nº 13.853, de 08 de julho de 2019, acrescentando artigos na LGPD e criando a ANPD.

Sendo a LGPD a lei principal relativa aos tratamentos de dados, cabe então uma análise específica sobre ela.

2.1.1 Lei Geral de Proteção de Dados Pessoais

A importância da proteção de dados pessoais aumenta à medida que a quantidade de dados criados e armazenados continua a crescer. No Brasil, o quadro jurídico em matéria de proteção de dados passou a ser repensado a partir do ponto de vista técnico da aplicabilidade da LGPD, além da perspectiva institucional, ou seja, através desse cenário organizações e tribunais estão desenhando novas linhas sobre a matéria, traçando um novo panorama acerca dos nortes gerais da proteção de dados pessoais e sua aplicabilidade.

A legislação nacional de proteção de dados pessoais oferece maiores garantias aos brasileiros, como os direitos dos titulares, bases legais para o tratamento, princípios norteadores, agentes de tratamentos, responsabilidade do responsável pelo tratamento, entre outros pontos.

É importante salientar as exceções nas quais a LGPD não será aplicada, conforme previsto no artigo 4º, de forma que ela não se aplica a tratamento de dados pessoais realizado por pessoa natural com fins exclusivamente particulares e não econômicos, ou que seja realizado com fins jornalísticos, artísticos ou acadêmicos[11].

A partir disso, a Lei Geral de Proteção de Dados Pessoais estabeleceu regras específicas para o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Essas regras visam garantir que, sempre que associado à produção e à disseminação do conhecimento, o tratamento de dados pessoais seja realizado com segurança jurídica e com respeito aos direitos dos titulares[12].

Nesta regulamentação busca-se equilibrar os princípios presentes na lei como o da privacidade e da autodeterminação informativa, a liberdade acadêmica e o livre fluxo de informações necessárias para a realização dos estudos e pesquisas, conforme disposto em guia emitido pela ANPD em 2023 com fins específicos de

---

[11] BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[12] ANPD. **Guia Orientativo. Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas.** 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf

orientar sobre o tratamento de dados pessoais para fins acadêmicos e para realização de estudos e pesquisa[13].

Atualmente, a proteção de dados pessoais pode ser analisada sob duas perspectivas, conforme ensina Renata Capriolli Zocatelli Queiroz[14]. Com relação à perspectiva da liberdade negativa, basta a simples garantia do direito de recusa ou de proibição por parte do titular do dado, enquanto na segunda, a proteção se estenderia para garantir o controle dos dados dos titulares, mesmo já possuindo domínio de terceiros sobre tais dados, ou seja, tratando-se da autodeterminação informativa.

A autodeterminação informativa, por sua vez, é o direito que cada indivíduo tem de controlar e proteger seus dados pessoais. É um dos fundamentos da disciplina de proteção de dados pessoais, conforme o art. 2º, inciso II, da LGPD, compreendido como forma de garantir o controle do cidadão sobre suas próprias informações. Objetiva-se, em última análise, assegurar que "*right data are used by the right people for the right purposes*"[15].

Em uma retomada histórica sobre o tema, importa citar que em 1967, em clássica obra ("*Privacy and Freedom*", Nova Iorque, Atheneum), Alan Westin advertia que, para manter a privacidade na era moderna, o indivíduo precisava ter a possibilidade de definir quando, como e quais as informações pessoais poderiam ser comunicadas a terceiros. Foi, entretanto, somente em dezembro de 1983 que esse aspecto da privacidade foi denominado de "direito à autodeterminação informativa" pelo Tribunal Constitucional da Alemanha, que declarou parcialmente inconstitucional uma lei, aprovada pelo parlamento em 1982, que disciplinava o censo populacional.

Havia, na época, previsão de uma ampla coleta de dados na Alemanha. De acordo com a lei questionada, aquele que se recusasse a responder a todas as perguntas teria que arcar com pesadas multas. A tentativa de disciplinarização não se limitava à elaboração de um quadro estatístico e demográfico, mas também à criação de um banco de dados para posterior confronto com outros já existentes nas agências federais e estaduais. Essa criação permitiria a correção de

---

[13] Op. Cit

[14] QUEIROZ, Renata Capriolli Zocatelli. **A proteção de dados pessoais**: a LGPD e a disciplina jurídica do encarregado de proteção de dados pessoais. 2021. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2021. Disponível em: https://doi.org/10.11606/T.2.2021.tde-23082022-085834.

[15] Paul Siehgart, Privacy and Computer, Londres: Latimer, 1976

dados armazenados anteriormente, bem como, a utilização de novas informações para objetivos específicos vinculados à natureza das agências.

A possibilidade de utilização de dados nessas circunstâncias gerou na opinião pública o temor de que as informações fossem utilizadas para controlar a atividade e comportamento dos cidadãos, gerando provocação da Corte Constitucional, que, em provimento cautelar, suspendeu a execução do recenseamento.

Em suma, apesar de algumas divergências conceituais, particularmente para eventual distinção em relação ao direito à proteção de dados, o direito à autodeterminação informativa decorre da Constituição Federal e da LGPD, e por não ser direito absoluto, pode sofrer restrição pelo legislador, desde que presente o interesse público ou outro direito de igual relevância[16].

Ele se aplica a tratamentos realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, uma vez que a LGPD é aplicável a operações de tratamento realizadas no território nacional[17].

Dentre esse robusto rol de princípios, destacam-se, para os fins deste trabalho, o da prevenção, o da responsabilização e prestação de contas. Além dos dispositivos mais prescritivos de comando e controle, como as obrigações específicas de atendimento aos direitos dos titulares, a previsão de tais princípios requer que os regulados adotem medidas ativas para prevenir o descumprimento da Lei, devendo esses agentes serem capazes de comprovar a adoção dessas ações.

Para além do princípio da responsabilização e prestação de contas, a LGPD também contempla dispositivos mais prescritivos no que se refere à obrigação dos agentes de tratamento de comprovarem o cumprimento da LGPD e de prevenir a ocorrência de danos. A título de exemplo, o art. 37 da Lei dispõe sobre a obrigatoriedade do controlador e do operador de manterem o registro das operações de tratamento de dados que realizarem. Além disso, o art. 38 prevê que a ANPD pode determinar que o controlador elabore relatório de impacto à proteção de dados

---

[16] BESSA, Leonardo Roscoe. A Lei Geral de Proteção de Dados e o direito à autodeterminação informativa. 2020. Disponível em: https://www.conjur.com.br/2020-out-26/leonardo-bessa-lgpd-direito-autodeterminacao-informativa/

[17] BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

pessoais.

Como já visto, a legislação brasileira sofreu grande influência da normativa europeia sobre proteção de dados, sendo importante visualizar as suas principais semelhanças e diferenças.

Uma vez que o GDPR precede a LGPD, tendo sido considerada legislação-base para a criação desta, importa analisar as semelhanças e divergências entre ambas no que se refere às bases da legislação que irão originar as demais normativas de proteção de dados.

Assim, destaca-se que a LGPD brasileira e o GDPR europeu compartilham diversas semelhanças, a exemplo:

> Ambas as leis aplicam-se não apenas às empresas e organizações estabelecidas em seus respectivos territórios, mas também às organizações localizadas fora de suas fronteiras, desde que processem dados de residentes do Brasil ou da União Europeia; tanto a LGPD quanto o GDPR estabelecem princípios-chave para o processamento de dados pessoais, como legalidade, lealdade, transparência, limitação de finalidade, minimização de dados, exatidão, limitação de armazenamento, integridade e confidencialidade. Ambas as legislações preveem a figura do controlador e do operador de dados e estabelecem suas responsabilidades e obrigações[18].

Ainda semelhantemente, ambas as leis exigem uma base legal para o tratamento de dados pessoais: o GDPR prevê seis bases legais, incluindo o consentimento, o cumprimento de obrigações legais, a execução de um contrato, a proteção de interesses vitais, o interesse público e o interesse legítimo. Por seu turno, a LGPD lista, a princípio, dez bases legais, que são similares às do GDPR, mas incluem algumas especificidades, como a proteção à saúde e a realização de estudos por órgãos de pesquisa[19]. Complementando as dez bases legais previstas no artigo 7º, também podemos citar as previstas no artigo 11 do mesmo diploma legal, quais sejam: quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; ou sem fornecimento de consentimento do

---

[18] COELHO, Pablo Martins Bernardi, et al. **Responsabilidade dos provedores pelo tratamento dos dados sensíveis – Uma visão de acordo com as Leis de Proteção de Dados brasileira e europeia**. 2024. Disponível em: https://revistas.unimilitar.edu.co/index.php/dere/article/view/7053/5841

[19] Op. Cit.

titular, nas hipóteses em que for indispensável.

Com relação a esta última possibilidade, será nas hipóteses em que for indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador; para o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e para a proteção da vida ou da incolumidade física do titular ou de terceiro.

Por fim, também poderá ter seu tratamento sem o fornecimento de consentimento do titular quando for indispensável para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais[20].

Sobre os princípios, no GDPR podem ser encontrados no capítulo 2, nos artigos 5 a 11, enquanto na LGPD constam no artigo 6º, incisos I a X. Em estreita análise, e a partir de uma leitura sistemática entre ambas as legislações, é possível identificar algumas equivalências, demonstradas na tabela abaixo:

Quadro 1: comparativo entre os princípios equivalentes da LGPD e GDPR

LGPD	**GDPR**
Princípio da transparência	Princípio da transparência
Princípio da finalidade	Princípio da limitação da finalidade
Princípio da segurança	Princípio da integridade
Princípio da qualidade de dados	Princípio da exatidão
Princípio da prevenção	Princípio da confidencialidade
Princípio da necessidade	Princípio da minimização dos dados

[20] Art. 11 da LGPD.

Fonte: A autora

Os demais princípios de ambas as legislações não possuem equivalência, tendo cada uma sua importância no que se refere a proteção de dados e ao tratamento exercido pelos agentes responsáveis.

O GDPR estabelece autoridades de proteção de dados em cada país membro da União Europeia e não unicamente uma supranacional. Assim, a referida legislação exige que os países membros da UE tenham autoridades de proteção de dados independentes. No Brasil, a LGPD pretendeu criar a Autoridade Nacional de Proteção de Dados (ANPD) por meio da Medida Provisória nº 869 de 27 de dezembro de 2019, a qual sofreu inúmeros vetos, sendo convertida na Lei nº 13.709, de 14 de agosto de 2018, criando de fato a ANPD e alterando dispositivos da LGPD.

De início, foi proposta como órgão da administração pública federal, mas foi transformada em autarquia com status de agência reguladora no ano de 2023 por meio do Decreto nº 11.348, de 01 de janeiro de 2023[21]. Assim, embora seja autônoma, não é completamente independente do Governo Federal[22].

No que se refere à exclusão de dados, tanto o GDPR quanto a LGPD autorizam que os titulares de dados solicitem a exclusão de suas informações pessoais, ressalvando as isenções previstas nos dois diplomas legais. Dentre as exceções, alguns são semelhantes entre si, quais sejam: quando o tratamento de dados pessoais é feito para fins de pesquisa, jornalísticos, artísticos ou acadêmicos, ou no cumprimento de obrigação legal[23].

Quanto ao acesso à informação: tanto o GDPR, quanto a LGPD, apresentam um elevado grau de semelhança no que diz respeito ao princípio da transparência, pois ambos os normativos exigem que os responsáveis pelo tratamento ou controlador enviem aviso ao titular de dado com informações detalhadas acerca do tratamento de seus dados pessoais[24].

Quanto à oposição ao tratamento de dados: tanto o GDPR, quanto a

[21] Art. 2º, IV, “b”, do Decreto nº 11.348, de 01 de janeiro de 2023.
[22] COELHO, Pablo Martins Bernardi, et al. **Responsabilidade dos provedores pelo tratamento dos dados sensíveis – Uma visão de acordo com as Leis de Proteção de Dados brasileira e europeia**. 2024. Disponível em: https://revistas.unimilitar.edu.co/index.php/dere/article/view/7053/5841
[23] Artigos 13 e 18 da LGPD e artigo 17 do GDPR
[24] Artigos 6, 9, 18 e 19 da LGPD e 12 e 15 do GDPR

LGPD, permitem que os titulares dos dados pessoais se oponham ao tratamento de seus dados[25].

Além dos pontos de convergência analisados acima, ambas as legislações possuem semelhanças no que se refere ao tratamento dos dados pessoais e aos seus agentes de tratamento, sobre os quais serão analisadas tais semelhanças nos tópicos próprios (subsequentes).

Por fim, apesar de a lei brasileira ter sofrido grande influência da legislação europeia, não são de todo convergentes, existindo divergências desde os princípios até a regulamentação sobre os responsáveis pelos tratamentos de dados.

E sobre os responsáveis pelo tratamento dos dados coletados, temos na LGPD duas figuras principais, as quais se dividem em operador de dados e controlador de dados.

Para uma melhor compreensão de como se dão esses tratamentos, é importante examinar a legislação de cada um, com uma análise mais aprofundada do operador de dados, começando pela revisão das definições de dado e sua relevância, a fim de estabelecer uma base para o tratamento dos dados pelo agente de tratamento.

[25] Artigo 15 da LGPD e artigos 7 e 21 do GPDR

3 AGENTES DE TRATAMENTO DE DADOS PESSOAIS

A respeito da revisão do conceito de dado pessoal, a LGPD define, em seu artigo 5º, o dado pessoal e o dado pessoal sensível. No inciso I, definem-se como dados pessoais aqueles que dizem respeito a uma pessoa natural identificada ou identificável. No inciso II, são considerados dados sensíveis aqueles relacionados à origem racial ou étnica, à convicção religiosa, à opinião política, à filiação a sindicato ou a organização de caráter religioso, filosófico ou político, à saúde ou à vida sexual, ao dado genético ou biométrico, quando vinculado a uma pessoa natural.

O GDPR possui definição semelhante, englobando dados sobre origem racial, opiniões políticas, convicções religiosas, filiação sindical, dados genéticos, biométricos, de saúde ou vida sexual. Ambas enfatizam a natureza delicada desses dados e a necessidade de proteção reforçada.

No inciso VIII do artigo 2º da Resolução CD/ANPD nº 18/2024, resta definido o tratamento de dados 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[26].

Tal definição encontra-se em consonância com a LGPD, de modo que o tratamento de dados corresponde a qualquer operação realizada em dados pessoais, seja ela coleta, produção, recebimento, classificação, uso, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, exclusão, avaliação ou controle da informação, modificação, comunicação, transferência, disseminação ou extração[27].

A definição se distingue pouco da trazida no ordenamento europeu, no qual se trata da coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou de outra forma disponibilização, alinhamento ou combinação,

[26] Op. Cit.
[27] Artigo 5º, inciso X da LGPD.

restrição, apagamento ou destruição[28].

Com as devidas exceções, é indispensável o consentimento expresso do titular dos dados para qualquer tipo de atividade de tratamento. Nesse sentido, Tarcisio Teixeira sustenta que o consentimento autoriza apenas o agente que o obteve, não se estendendo a outros agentes. Para isso, é necessário obter o consentimento expresso do titular do dado para o compartilhamento[29].

A LGPD determina que os dados pessoais devem ser tratados para propósitos legítimos, específicos, explícitos e informados ao titular. A partir deste enunciado, é possível notar que a atividade de tratamento de dados pessoais deve estar atrelada a uma finalidade específica, ou seja, cabe ao agente de tratamento identificar o grau de utilidade do dado pessoal para atingir a finalidade especificada e, consequentemente, estabelecer o grau necessário de anonimização dos dados.

Sobre tais agentes, são apresentados pela LGPD como o controlador e o operador, não sendo enquadrado como agente de tratamento a figura do encarregado, denominado no GDPR como DPO (*Data Protection Officer*). Contudo, a fim de definir a atuação de cada um, importa também entender a figura do encarregado de dados, sem, entretanto, esgotar o assunto.

Assim, em uma comparação entre ambas as normas, temos três figuras e destaque: o responsável pelo tratamento (*Controller*), o subcontratante (*Processor*) e o encarregado da proteção de dados (*Data Protection Officer ou DPO*) no GDPR, os quais também são encontrados na LGPD, sendo eles o controlador, o operador, e o encarregado, com a observação de que o responsável pelo tratamento corresponde ao controlador e o subcontratante equivale ao operador, sendo a figura do encarregado a mesma do DPO no GDPR.

A LGPD traz em seu capítulo VI sobre os agentes de tratamento de dados pessoais, iniciando na seção I o destaque sobre o controlador e o operador, nos artigos 37 a 40, como será visto na sequência. Já a figura do encarregado é tratada no capítulo VII, mais especificamente no artigo 41.

O encarregado, ou DPO como é denominado pelo GDPR, é indicado

---

[28] Artigo 4º, nº 2º e considerando 15, do GDPR. UNIÃO EUROPÉIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT.

[29] TEIXEIRA, Tarcisio, et al. **Lei Geral de Proteção de Dados Pessoais: comentada artigo por artigo**. 4. Ed. São Paulo: SaraivaJur, 2022.

pelo controlador, e no exercício de suas atribuições pode desempenhar o papel de fomentar e disseminar a cultura de proteção de dados pessoais na organização em que exerce suas funções, sendo dispensado a sua indicação para empresas de pequeno porte[30].

Sobre a figura do DPO, mesmo este não se enquadrando como agente de tratamento de dados, cumpre esclarecer suas atribuições, para diferenciação do seu papel e dos agentes de tratamento. O Ministério da Justiça e Segurança Pública, juntamente com a ANPD e o Conselho diretor, aprovaram a Resolução CD/ANPD nº 18, de 16 de julho de 2024, trazendo um novo regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais, a qual entrou em vigor na data de 17 de julho de 2024.

Nas disposições preliminares, é esclarecido que se trata de normas complementares sobre a indicação, a definição, as atribuições e a atuação do encarregado, já tratada na LGPD. É certo que cabe ao encarregado aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências cabíveis; receber comunicações da ANPD e adotar providências cabíveis; orientar os funcionários e os contratados do agente de tratamento a respeito das práticas a serem tomadas em relação à proteção de dados pessoais e executar as demais atribuições determinadas pelo agente de tratamento ou estabelecidas em normas completares.

Contudo, como ressaltado, os agentes de tratamento são o controlador e o operador, não se encaixando o DPO como um agente de tratamento, de forma que cumpre a análise dos referidos agentes e suas atribuições com relação ao processo de tratamento de dados pessoais.

Assim, retornando ao tema a respeito dos agentes de tratamento, são estabelecidos os seus deveres, evidenciando que deverão prover os meios necessários para o exercício das atribuições do encarregado, neles compreendidos, entre outros, recursos humanos, técnicos e administrativos.

Deve o agente de tratamento, ainda, assegurar aos titulares meios céleres, eficazes e adequados para viabilizar a comunicação com o encarregado e o

---

[30] ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf.

exercício de direitos, e garantir ao encarregado acesso direto às pessoas de maior nível hierárquico dentro da organização, aos responsáveis pela tomada de decisões estratégicas que afetem ou envolvam o tratamento de dados pessoais, bem como às demais áreas da organização.

Voltando-se especificamente aos agentes, já restou claro que se dividem (no ordenamento brasileiro) em operador e controlador. O controlador de dados pode ser qualquer pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, conforme preconiza o artigo 5º, inciso VI da Lei 13.709/18[31]. É o agente que decide como e porque os dados serão coletados e tratados, não sendo necessariamente aquele quem coleta tais dados.

Um dos documentos utilizados pelo menos é o relatório de impacto a proteção de dados pessoais, o qual contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, além de medidas, salvaguardas e mitigação de riscos, possuindo ainda a obrigação de manter registro das atividades de tratamento de dados que realizam.

Ainda, cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com as normativas da Lei Geral de Proteção de Dados Pessoais. O controlador irá fornecer instruções ao operador para que este realize a atividade de tratamento, passando então a análise desta figura tão importante.

3.1 Operador de Dados

O operador de dados é um agente de tratamento e pode ser qualquer pessoa natura ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, conforme inciso VII do art. 5º da LGPD.

A Autoridade Nacional de Proteção de Dados emitiu um Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, o qual se encontra atualmente na sua segunda versão, emitida em abril de 2022[32].

---

[31] BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[32] ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do**

No referido guia vislumbra-se a figura do operador de dados com a mesma definição acima, complementada pelo previsto no artigo 39 da mesma lei, o qual ensina que “o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria”.

Desta forma, nota-se que o operador deverá agir nos limites das finalidades decretadas pelo controlador, possuindo liberdade na escolha dos meios de tratamento de dados, mas não com relação às finalidades, não possuindo ainda aquele o poder de decisão, ao contrário deste. Outro ponto importante é que o operador deverá, necessariamente, ser uma pessoa diversa do controlador, que não atue como subordinado ao mesmo ou como um membro do seu órgão.

Na relação entre controlador e operador, com implementação prática no GDPR, pode-se verificar o *Data Processing Agreement*, um documento essencial que descreve os termos e condições para o tratamento de dados pessoais. É um contrato entre o controlador e o operador que descreve as funções e responsabilidades das partes quando os dados pessoais são tratados.

Ele precisa satisfazer uma série de requisitos para estar em conformidade com as leis de privacidade de dados, incluindo o Regulamento Geral de Proteção de Dados[33]. É considerado um dos passos mais básicos para se estar em conformidade com o regulamento europeu, existindo um modelo para tal contrato no site GDPR.EU[34].

No contrato restam descritas definições e interpretações, atribuições atinentes ao operador e ao controlador, termos gerais como o de confidencialidade, consentimento com as leis existentes, e assinatura com nome, data e outras informações que as partes acharem necessárias. Serve tal contrato para reforçar a relação entre controlador e operador nos processos de tratamento de dados, e que ambos devem agir conforme os ditames legais.

Ainda conforme o Guia Orientativo, sobre a responsabilidade do operador, tem-se que muito embora o controlador tenha a principal responsabilidade

---

Encarregado. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf.

[33] STRIPE. **Data Processing Agreement – FAQS**. Disponível em: https://stripe.com/br/legal/dpa/faqs

[34]GDPR.EU. **Data Processing Agreement (Template).** Disponível em: https://gdpr.eu/data-processing-agreement/

e o operador deva atuar em nome dele, o art. 37 da LGPD determina que ambos partilham obrigações e, consequentemente, a responsabilidade de manter o registro das operações de tratamento. Além disso, nos termos do art. 42 da LGPD, ambos possuem a obrigação de reparação se causarem dano patrimonial, moral, individual ou coletivo a outrem, no âmbito de suas respectivas esferas de atuação.

Contudo, via de regra, as obrigações e responsabilidades do controlador e do operador são distintas, por serem determinadas conforme o papel exercido por cada um no âmbito do tratamento dos dados pessoais. Assim, a responsabilidade solidária estabelecida pelo inciso I, § 1º do art. 42 da LGPD, prevista para os casos de danos causados em razão do tratamento irregular realizado por operador (por descumprir as obrigações da legislação ou por não observar as instruções do controlador), pode ser considerada uma excepcionalidade, já que em regra a responsabilidade é do controlador. Em princípio, essa é a única hipótese em que o operador é equiparado ao controlador[35].

O operador de dados possui responsabilidade de manter o registro das operações de tratamento realizadas, e apesar de, geralmente, a responsabilidade ser do controlador, ela poderá ser solidária quando ele descumprir obrigações impostas pela legislação. Apesar de a legislação não prever a existência do suboperador, a ANPD deixa claro que não há vedação para que o operador de dados contrate um auxiliar a fim de realizar o tratamento de dados pessoais em conjunto, sempre em nome do controlador.

Ao contrário da LGPD, no GDPR, há a previsão legal da figura do subcontrolador em seu artigo 28, embora não haja uma definição específica. É importante salientar que, quando o tratamento dos dados é realizado por sua conta, o responsável pelo tratamento recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de forma a atender aos requisitos atuais.

Na legislação europeia, o subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral. Em caso de autorização geral por escrito, o

---

[35] ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf.

subcontratante informa o responsável pelo tratamento de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratantes, dando assim ao responsável pelo tratamento a oportunidade de se opor a tais alterações.

O tratamento em subcontratação é regulado por contrato ou outro ato normativo ao abrigo do direito da União, ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento.

No artigo 4º do GDPR, que traz os conceitos legais semelhantes ao disposto no artigo 5º da LGPD, existe a definição da figura do "*processor*" como sendo "uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes". Essa figura poderia muito bem servir para qualificação dos empregados de uma empresa, que fazem o tratamento de dados em nome do empregador, se não fosse a ressalva feita no artigo 29 da mesma lei.

Segundo o Professor Menezes Cordeiro[36], o subcontratante é um mandatário do responsável pelo tratamento, atua por conta deste último. O subcontratante será ainda, por maioria de razão, titular de uma posição fiduciária: está obrigado a atuar sempre no melhor interesse do beneficiário da relação, qual seja, o responsável pelo tratamento.

Não há relação direta entre o suboperador e o controlador, como ocorre no caso do operador, contudo tanto o operador quanto o suboperador poderão responder perante a ANPD, uma vez que este pode ser equiparado àquele perante a LGPD em relação às atividades que foi contratado para executar.

Em termos de competências, atividades, obrigações e aspectos jurídicos peculiares sobre os operadores na LGPD pode-se citar a designação de DPO (art. 5º, inc. VIII); a garantia de adoção das medidas técnicas e administrativas pertinentes para o cumprimento dos princípios gerais de proteção e dos direitos do

---

[36] MENEZES CORDEIRO, A. Barreto. **Direito da proteção de dados: à luz do RGPD e da Lei 58/2019.** Coimbra: Almedina, 2020.

titular no âmbito da transferência internacional de dados pessoais (art. 35, § 5º); obrigação de manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse (art. 37); etc.

Ainda incumbe ao operador realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria (art. 39).

O operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (art. 42), e neste sentido, quando não tiver seguido as instruções lícitas do controlador, o operador responde solidariamente pelos danos causados pelo tratamento, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 da LGPD (art. 42, § 1º, inc. I).

O operador responde pelos danos decorrentes da violação da segurança dos dados, se tiver deixado de adotar as medidas de segurança previstas no art. 46 da LGPD, e isso der causa a dano (art. 44, parágrafo único), devendo adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito (art. 46).

Em suas atribuições, precisa a segurança da informação prevista na LGPD em relação aos dados pessoais, mesmo após o seu término (art. 47), assim como formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (art. 50).

Ao estabelecer tais regras, o operador considerará, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular (art. 50, § 1º).

É importante salientar que, em caso de infração às normas da LGPD, as punições podem ser de advertência, com indicação de prazo para adoção de medidas corretivas, e de multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no último exercício, excluídos os tributos, limitadas a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

Pode ser ainda de multa diária, observado o limite total a que se refere o inciso II do art. 52 da LGPD; 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; e eliminação dos dados pessoais a que se refere a infração.

Pode ocorrer também a suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) 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 (seis) meses, prorrogável por igual período; e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (art. 52);

Assim, não cumpridas as finalidades de tratamento dos dados coletados por parte do operador, não respeitados os princípios referentes a proteção de dados ou ocorrido alguma das hipóteses previstas na LGPD e na regulamentação da dosimetria de sanções, implica ao operador o resultado de condutas lesivas quando do tratamento dos dados, mesmo sendo o controlador o responsável direto.

Para tanto, importa analisar alguns exemplos de incidentes de dados, a fim de compreender de que forma pode ocorrer um incidente de segurança, seja ele um vazamento de dados ou não, para um maior aprofundamento do papel do operador neste processo de tratamento de dados.

4 INCIDENTES DE SEGURANÇA E VAZAMENTOS DE DADOS

Quando se fala em violação de dados ou *data breach*, significa que os dados confidenciais e sensíveis foram disponibilizados a uma pessoa não autorizada. O *data breach* ou atentado de dados pessoais é, conforme conceituação da União Europeia, uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento[37].

Conforme a definição da ANPD, um incidente de segurança com dados pessoais é qualquer evento adverso que seja confirmado, relacionado à violação da segurança de dados pessoais, como o acesso não autorizado, acidental ou ilegal, que resulte na destruição, perda, alteração, vazamento ou qualquer outra forma de tratamento de dados inadequada ou ilícita, que possa representar um risco para os direitos e liberdades do titular dos dados[38].

O vazamento de dados pessoais, um dos mais conhecidos incidentes de segurança, ocorre quando dados são indevidamente acessados, coletados e divulgados ou repassados a terceiros. O dano ao titular pode ser das mais diversas naturezas, como fraudes, tentativas de golpes, uso indevido dos dados, venda dos dados, etc.

Um dos incidentes de segurança que culminou uma evolução no que tange aos vazamentos de dados pessoais foi o da Carolina Dieckmann em maio de 2011. Um hacker invadiu o computador pessoal da atriz, possibilitando o acesso a 36 fotos pessoais de cunho íntimo. De acordo com a denúncia, o invasor exigiu R$ 10 mil para não publicar as fotos[39]. Como a atriz recusou a exigência, acabou tendo suas fotos divulgadas na internet. Isso criou uma grande discussão popular sobre a criminalização desse tipo de prática, que ainda foi excessivamente fomentada pela

---

[37] União Europeia. (2016) Regulamento Geral sobre a Proteção de Dados. Regulamento 2016/679 do Parlamento Europeu e do Conselho. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FUL-L&from=EN

[38] GOV. **Incidentes de segurança com dados pessoais**. 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/semana-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais

[39] G1. Suspeitos do roubo das fotos de Carolina Dieckmann são descobertos. 2012. Disponível em: https://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html

mídia. A atriz abraçou a causa e cedeu seu nome à Lei nº 12.737/2012, o primeiro texto que tipificou os crimes cibernéticos, tendo foco nas invasões a dispositivos que acontecem sem a permissão do proprietário.

Outro ataque que ficou mundialmente conhecido foi o ocorrido em 2014 como Facebook/Cambridge Analytica. A Cambridge Analytica valeu-se de informações básicas (nome, profissão, cidade) e de hábitos e preferências políticas de 50 milhões usuários do Facebook para a realização não autorizada de testes comportamentais, que futuramente foram utilizados na campanha presidencial do ex-presidente dos EUA, Donald Trump, e na votação do Brexit[40].

No mesmo ano, um vazamento de dados expôs as contas de 145 milhões de usuários (nomes, endereços, datas de nascimento e senhas criptografadas) da eBay, uma das maiores empresas de comércio eletrônico do mundo. Segundo a empresa, hackers usaram as credenciais de três funcionários para acessar sua rede e tiveram livre acesso ao banco de dados dos usuários por 229 dias[41].

Em dezembro de 2020, reportagem do jornal O Estado de S. Paulo revelou que dados de 243 milhões de brasileiros cadastrados no Sistema Único de Saúde (SUS) ou como beneficiários de planos de saúde ficaram expostos na internet por falhas de segurança do Ministério da Saúde. As informações que ficaram expostas na internet, como nome completo, CPF, endereço e telefone, deveriam estar protegidas por login e senha, mas havia uma vulnerabilidade no código que permitia que qualquer usuário consultasse o banco de dados[42].

O Banco Central comunicou no dia 21 de janeiro de 2024 um incidente de segurança com vazamento de dados pessoais vinculados às chaves PIX que estavam sob a guarda e a responsabilidade da empresa Acesso Soluções de Pagamento.

Os dados de 160.147 chaves foram potencialmente expostos. Foram

---

[40] BBC. **O escândalo que fez o Facebook perder US$ 35 bilhões em horas**. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43466255

[41] G1. **Site eBay é vítima de ciberataque e recomenda mudança de senha.** 2014. Disponível em: https://g1.globo.com/tecnologia/noticia/2014/05/site-ebay-e-vitima-de-ciberataque-e-recomenda-mudanca-de-senha.html

[42] ARAGÃO, Alexandre. **5 grandes vazamentos de dados no Brasil — e suas consequências**. 2022. Disponível em: https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022

informações como nome completo, CPF, instituição, número da agência e conta. O fato ocorreu entre 3 e 5 de dezembro de 2021. De acordo com a nota do Banco Central, não foram expostos dados sensíveis, como senhas, extratos ou outras informações sob sigilo bancário. No mesmo ano ainda houve novo vazamento relacionado a chaves PIX, desta vez da Quesh Instituição de Pagamento, onde vazaram dados cadastrais vinculados a 53.383 chaves PIX[43].

Atualmente, foi constatado um aumento considerável do número de casos de vazamentos de dados, e isto considerando-se só a primeira metade de 2024, segundo relatório do Centro de Recursos para Roubo de Identidade (ITRC, na sigla em inglês). Ao todo, foram 1,1 bilhão de casos, representando um aumento de 490% em comparação ao primeiro semestre de 2023. Já ao se considerar o número de vítimas afetadas pelos vazamentos, os números ficam ainda maiores, sendo um bilhão, no segundo trimestre de 2024, significando um aumento de 1.170% em comparação ao mesmo período de 2023[44].

Ainda sobre vazamentos ocorridos recentemente, em 29 de maio de 2024, houve um vazamento de dados do Google, em que foram expostos cerca de 2.500 documentos internos da empresa. Entre os documentos, estavam mais de 14 mil algoritmos de classificação e informações sobre como o Google coleta dados e como funcionam os resultados de pesquisa.

O vazamento de dados do Google revelou que o Google dá preferência a sites que otimizam o SEO, e usa dados do Chrome para ver como os usuários interagem com os resultados de busca. Verifica se as pessoas estão clicando no seu link e passando tempo no seu site, enviando um sinal positivo para o Google, e ranqueia páginas com base em dados dos sites, como o número de cliques, e dados dos usuários do Chrome[45].

Os sites populares com muitos acessos podem ser mostrados

---

[43] MARTELLO, Alexandre. **Banco Central comunica vazamento de dados de 53 mil chaves PIX da Qesh Instituição de Pagamento**. 2024. Disponível em: https://g1.globo.com/economia/noticia/2024/09/30/banco-central-comunica-vazamento-de-dados-de-53-mil-chaves-pix-da-qesh-instituicao-de-pagamento.ghtml

[44] SPADONI, Pedro. **Vazamentos de dados atingem patamares assustadores em 2024, alerta relatório**. 2024. Disponível em: https://olhardigital.com.br/2024/07/18/seguranca/vazamentos-de-dados-atingem-patamares-assustadores-em-2024-alerta-relatorio/

[45] SILVEIRA, Julia. **Documentos vazados mostram como o algoritmo do Google funciona; entenda**. 2024. Disponível em: https://www.techtudo.com.br/noticias/2024/06/documentos-vazados-mostram-como-o-algoritmo-do-google-funciona-entenda-edsoftwares.ghtml

primeiro no ranking de buscas, mesmo que sites desconhecidos tenham informações de melhor qualidade.

O vazamento dos documentos foi descoberto pelo profissional de SEO e fundador da EA Eagle Digital, Erfan Azimi no início de maio, e confirmado publicamente pelo Google no dia 29 do mesmo mês[46].

Azimi disse que não tinha motivos financeiros para apontar o vazamento. Ele afirmou que seu principal motivo era fazer com que "a verdade fosse revelada". No entanto, Azimi não teria sido o responsável direto pelos vazamentos.

Não está totalmente claro como as informações chegaram a público, mas o site Entrepreneur aponta que o vazamento pode ter ocorrido quando o Google publicou acidentalmente os documentos internos no GitHub, de propriedade da Microsoft, em março[47].

As escolhas que o Google faz nas pesquisas têm um impacto profundo em qualquer pessoa que dependa da Web para fazer negócios, desde pequenos editores independentes a restaurantes e lojas online. Por sua vez, surgiu uma indústria de pessoas que esperam decifrar o código ou ser mais espertos que o algoritmo, fornecendo respostas por vezes contraditórias.

As informações tornadas públicas provavelmente causarão repercussões nos setores de otimização de mecanismos de pesquisa (SEO), marketing e publicação.

Também em 2024, houve um vazamento significativo, este em janeiro, o qual ficou conhecido como “*Mother of All Breaches (MOAB)*”, o que em uma tradução livre significa “a mãe de todas as violações”. Com 12 terabytes de informações abrangendo impressionantes 26 bilhões de registros, este vazamento supermassivo contém dados de uma variedade de fontes. O maior número de registros no MOAB, 1,4 bilhão, veio do aplicativo chinês de mensagens instantâneas Tencent QQ. O vazamento também incluiu centenas de milhões de registros de plataformas como Weibo, MySpace, Twitter, Deezer, LinkedIn, AdultFriendFinder, Adobe, Canva, VK, Daily Motion, Dropbox e Telegram, além de várias organizações governamentais em países como EUA, Brasil, Alemanha, Filipinas e Turquia[48].

---

[46] Op. Cit.
[47] Op. Cit.
[48] XAVIER, Fábio Correa. **Mãe de Todas as Violações: Entendendo o Maior Vazamento de Dados**

Os registros incluem uma grande variedade de informações pessoais e confidenciais, aumentando exponencialmente o risco de ataques de identidade, phishing sofisticado, ciberataques direcionados e acesso não autorizado a contas pessoais e sensíveis. Além disso, o MOAB contém não apenas informações de violações anteriores, mas também novos dados, aumentando a preocupação sobre a segurança e a privacidade dos dados na internet.

Um banco de dados chamado "RockYou2024" foi vazado no dia 4 de julho de 2024. As informações sensíveis não estão criptografadas. O vazamento adicionou 1,5 bilhão de novas senhas a outras publicações, totalizando agora 9.948.575.739 de senhas divulgadas. O responsável pela publicação do conteúdo foi um hacker usando o nome "ObamaCare"[49].

O conjunto foi descoberto em um fórum de hackers e divulgado pelo site Cybernews. Segundo a Cybernews, o vazamento representa "perigos severos para usuários propensos a reutilizar senhas". O portal afirma que o compilado traz senhas usadas por pessoas de todo o mundo, o que pode levar ao crescimento do número de fraudes e ataques virtuais, além de crimes ligados à identidade.

Há três anos, a Cybernews também publicou sobre o vazamento do banco de dados chamado "RockYou2021", o qual fora o maior vazamento até então, expondo 8,4 bilhões de senhas em texto simples. O novo vazamento de 2024 seria uma extensão daquele[50].

Ainda em julho de 2024, especificamente no dia 10, o Banco Central (BC) informou a ocorrência de um vazamento de dados de um total de 39.088 chaves Pix de clientes da 99Pay Instituição de Pagamentos. Segundo o BC, o vazamento ocorreu de 26 de junho e 2 de julho e abrangeu o nome do usuário, o Cadastro de Pessoa Física (CPF) com máscara (CPF com asteriscos para não mostrar todos os números), a instituição de relacionamento, a agência e o número da conta, ocorrendo devido a falhas pontuais em sistemas da instituição de pagamento. A exposição ocorreu em dados cadastrais, que não afetam a movimentação de dinheiro. Dados

---

da História. 2024. Disponível em: https://securityleaders.com.br/mae-de-todas-as-violacoes-entendendo-o-maior-vazamento-de-dados-da-historia/

[49] TILT. **9,9 bi de senhas divulgadas: vazamento pode ser um dos maiores da história**. 2024. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2024/07/12/novo-vazamento-de-senhas-pode-ser-um-dos-maiores-da-historia.htm

[50] Op. Cit.

protegidos pelo sigilo bancário, como saldos, senhas e extratos, não foram expostos[51].

Os exemplos acima citados são apenas alguns dos grandes incidentes de segurança acontecidos, que trazem em tela a importância da atuação dos agentes de tratamento para que tais incidentes não ocorram.

O art. 46 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) determina que os agentes de tratamento de dados pessoais devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito[52].

Claramente nem todos os incidentes de segurança e vazamento de dados ocorrem somente por erro dos agentes de tratamento, contudo eles têm que observar os procedimentos adequados desde o momento da coleta dos dados, para minimizar os riscos de qualquer intercorrência, e agir conforme o necessário quando do vazamento dos dados tratados.

---

[51] MÁXIMO, Wellton. **Banco Central comunica vazamento de dados de 39 mil chaves Pix**. 2024. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2024-07/banco-central-comunica-vazamento-de-dados-de-39-mil-chaves-pix

[52] BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

5 ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS

A segurança da informação pode ser traduzida como a proteção das informações importantes de uma organização -arquivos e dados digitais, documentos em papel, mídia física e até mesmo fala humana -contra acessos, divulgação, uso ou alteração não autorizados. A segurança da informação digital também é chamada de segurança de dados[53].

A prática de segurança da informação é fundamentada na tríade CIA ("Confidentiality", "Integrity" e "Availability"), que corresponde à sigla CID em português (Confidencialidade, Integridade e Disponibilidade), e se destina a orientar a escolha de tecnologias, políticas e práticas das organizações para proteger seus sistemas de informação (hardware, softwarebem como as pessoas envolvidas na produção, armazenamento, uso e troca de dados dentro da tecnologia da informação da empresa (TI) a infraestrutura)[54]. A política de segurança da informação envolve a o tratamento efetivo desses dados, sua operação e manutenção.

Para Hintzbergen, a segurança da Informação pode ser traduzida na “preservação da confidencialidade, integridade e disponibilidade da Informação”, acrescentando ainda que, “adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, também podem ser incluídas”[55].

Quando falamos em anonimização e pseudonimização de dados, impossível dissociar o caráter do direito do caráter da tecnologia da informação. Sobre a tecnologia da informação, conforme ensina Tarcisio Teixeira, o seu uso de modo geral, a exemplo da internet, celular, entre outros, “tem sido para muitos um fim em si mesmo, não um meio que facilite as atividades cotidianas e permita maior interação humana”. Para o autor, ao contrário disto, a tecnologia promove o afastamento, o

---

[53] SILVA, Salvador Márcio Rodriguesda; GOMES, Ana Carolina Nogueira; NAZARÉ, Tiago Bittencourt. **Lei Geral de Proteção de Dados: Métodos de Anonimização e Pseudonimização**. 2023. Disponível em: https://periodicos.unis.edu.br/mythos/article/view/804

[54] Op. Cit.

[55] HINTZBERGEN, Kees; HINTZBERGEN, Jule; BAARS, Hans. **Fundamentos de Segurança da Informação: com Base na ISO 27001 e na ISO 27002**. 1. ed. São Paulo: Brasport, 2018

egoísmo, impedindo o compartilhamento e o companheirismo. “Assim, mais difícil para o ser o humano desenvolver-se e aprimorar-se como ser social que é"[56].

No que se refere especificamente aos dados, conjuntos de dados podem conter identificadores que possibilitam a associação, direta ou indireta, a um indivíduo, nos termos do art. 5º, XI e art. 12, § 4º, da LGPD. Daí se dizer que os identificadores podem ser diretos ou indiretos. O Identificador direto é o dado que por si só permite identificar unicamente uma pessoa natural, sem a necessidade de combiná-lo com dados de outras fontes como, por exemplo, o seu CPF.

Já o identificador indireto, por sua vez, é considerado o dado que por si só não tem a capacidade de identificar alguém, mas pode ser agregado e vinculado a dados auxiliares para identificar uma pessoa natural, a exemplo da nacionalidade, da idade, da raça, do CEP da residência, das características fenotípicas, ou do endereço de IP que podem ser necessários para distinguir alguém.

A Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), com o objetivo de definir fundamentos e promover a cultura de proteção de dados no Brasil, faz menção a processos que, mediante diferentes técnicas, possibilitam de algum modo afetar a vinculação do dado pessoal, de forma direta ou indireta, com o indivíduo, como as utilizadas em processos de anonimização e de pseudonimização.

Ensina Tarcicio Teixeira ainda que o dado pessoal trazido pela legislação brasileira não se refere somente a uma pessoa natural identificada, mas também a identificável. Alguns dados pessoais são capazes de identificar um indivíduo a depender das circunstâncias em que são utilizados, tratando-se dos já citados dados pessoais indiretos, o que por ter essa capacidade de identificar um indivíduo o confere a característica de dado pessoal[57].

Sobre os dados anônimos, o autor ainda cita que dados anônimos são dados pessoais e, portanto, tutelados pela LGPD. Por sua sorte, dados anonimizados se trata dos que, mediante técnicas como a criptografia, não possam ser levados a identificar uma pessoa.

---

[56] TEIXEIRA, Tarcisio. **Curso de Direito e Processo Eletrônico: doutrina, jurisprudência e prática**. 4. ed. São Paulo: Saraiva, 2018

[57] TEIXEIRA, Tarcisio, et al. **Lei Geral de Proteção de Dados Pessoais: comentada artigo por artigo**. 4. Ed. São Paulo: SaraivaJur, 2022.

Quando o dado for identificado através de meios razoáveis e disponíveis quando do tratamento dele, possibilitando-se a sua reidentificação, ocorrerá a pseudonimização.

Neste sentido, um estudo preliminar foi realizado pela ANPD sobre anonimização e pseudonimização para a proteção de dados pessoais, em dezembro de 2023. Quanto a sua estrutura, o referido estudo está organizado dividindo-se em conceitos básicos, processos de anonimização e pseudonimização de dados na LGPD e considerações finais. Possui ainda elementos complementares elencados em apêndices.

Em diferentes disposições da LGPD há indicações para a aplicação dos processos de anonimização ou de pseudonimização. Durante e depois do tratamento dos dados, em situações específicas, no tratamento e utilização de dados pessoais, é aplicável um desses processos para garantir ao titular a proteção contra o uso indevido ou abusivo dos seus dados pessoais.

A anonimização e a pseudonimização consistem, basicamente, na modificação ou destruição de informações em bases de dados, não tornando mais possível a identificação dos indivíduos, o que, geralmente, é realizado de três formas: supressão (alguns tipos de dados são eliminados da base de dados), substituição (dados são substituídos por outros dados ou dados falsos) e generalização (dados específicos são substituídos por categorias mais genéricas como quando a idade de indivíduos é substituída por intervalos. Por exemplo: “de x a x” anos)[58].

Há recomendação para uso da anonimização e da pseudonimização quando do tratamento de dados pessoais para realização de estudos por órgãos de pesquisa (art. 7º, IV) e no campo da saúde pública (art. 13, caput), em casos em que o controlador deseja conservar os dados para uso posterior e como um direito que o titular de dados possui, respectivamente, podendo requerer do controlador a anonimização de seus dados pessoais, quando esta é viável.

---

[58] SOUSA, Thiago do Rego; COUTINHO, Murilo; COUTINHO, Lilian; ALBUQUERQUE, Robson. **LGPD: Levantamento de Técnicas Criptográficas e de Anonimização para Proteção de Bases de Dados**. Sociedade Brasileira de Computação (SBC). 2020. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/19227/19056.

5.1 ANONIMIZAÇÃO

A anonimização é definida como a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. No mesmo sentido, dado anonimizado é definido como o relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Anonimização não torna os dados inúteis, ao contrário, um processo adequado de anonimização mantém os dados funcionais para um determinado propósito de tratamento e finalidades específicas.

Ao contrário deste, a LGPD, no § 4º do seu art. 13, trata da pseudonimização, do qual se extrai que o dado pseudonimizado é o que perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

A reidentificação, por seu turno, é o processo de tentar discernir os identificadores removidos dos dados desidentificados, inclusive a partir de técnicas de anonimização de dados[59]. Assim, a reidentificação pode transformar dados anonimizados em dados pessoais por meio do uso, por exemplo, de correspondência de dados ou técnicas semelhantes.

Os dados anonimizados não são considerados dados pessoais, por isso não estão sujeitos à proteção da LGPD, salvo quando o processo de anonimização a que foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

No caso do processo de anonimização, os dados são modificados de tal forma que se reduz substancialmente o risco de vinculá-los novamente à pessoa natural identificada ou identificável, mesmo com o uso de dados auxiliares. A remoção dos identificadores mediante esse processo torna tais dados como não pessoais para qualquer entidade, inclusive para o controlador dos dados.

Já na pseudonimização, embora a associação direta seja inicialmente

---

[59] GARFINKEL, Simson L. **De-Identification of Personal Information**. [S.l.]: National Institute of Standards and Technology, 2015. p. 9.

obscurecida, existe a possibilidade de reverter esse processo mediante o uso de informações adicionais mantidas separadamente pelo controlador em um ambiente controlado e seguro. Essas informações adicionais, sob controle estrito, são essenciais para reestabelecer a ligação entre os dados pseudonimizados e a identidade do titular de dados.

Ambos os processos buscam atender aos preceitos de proteção da privacidade e de proteção dos dados pessoais. Contudo, a pseudonimização, por permitir a reversibilidade do processo pelo controlador, demanda uma gestão cuidadosa das informações adicionais utilizadas para essa finalidade. É crucial que essas informações sejam mantidas em um ambiente seguro e controlado, evitando qualquer possibilidade de acesso não autorizado que possa comprometer a privacidade dos titulares de dados. Dessa forma, a escolha entre anonimização e pseudonimização dependerá da necessidade de preservação da privacidade e da reversibilidade dos dados no contexto específico de tratamento, considerando a finalidade, a utilidade dos dados e os riscos envolvidos no processo.

No estudo preliminar, é apresentada uma tabela com situações e aplicações de tais técnicas na LGPD:

Figura 1: Situações e aplicações da anonimização e pseudonimização na LGPD

Situações e Aplicação das técnicas na LGPD	Processo
Condicionante para o tratamento nas hipóteses do uso dos dados pessoais e dados pessoais sensíveis em pesquisas – art. 7º, inciso IV; art. 11, alínea "c" do inciso II;	Anonimização
Reversão do processo de anonimização – art. 12, *caput* e §§ 1º e 3º;	Anonimização
Tratamento de dados sensíveis – estudos e pesquisas em saúde pública – art. 13, *caput* e § 4º.	Pseudonimização
Conservação dos dados após o término do tratamento – *caput* no art. 16, incisos II e IV;	Anonimização
Direito dos titulares no art. 18, inciso IV; **compartilhamento e da portabilidade de dados** - § 6º e 7º do art. 18.	Anonimização

Fonte: Estudo preliminar, 2023[60].

Consistindo a anonimização de dados em um processo de remoção de identificadores diretos e indiretos, os dados pessoais submetidos ao processo de

[60] ANPD. **ESTUDO PRELIMINAR. Anonimização e Pseudonimização para a proteção de dados pessoais**. 2023. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/37060

anonimização devem ser, na origem, objeto de legítimo tratamento pelo agente responsável.

Neste sentido, é primordial que esteja em consonância com os princípios de proteção de dados, em todas as etapas de desenvolvimento da anonimização, em especial quanto aos princípios da finalidade, adequação e necessidade.

É imperioso ressaltar que dados anteriormente considerados pessoais, mas que foram submetidos a um processo de anonimização deixam de estar sujeitos ao escopo de aplicação da LGPD[61].

Conforme pode ser extraído de uma leitura analítica do artigo 12 da LGPD, este processo seria um conjunto de atos ou medidas entre si relacionadas, iniciando-se com o processamento de dados pessoais, e aplicando-se então técnicas variadas para desassociar identificadores do dado em seu estado originário ou bruto[62].

Ainda em estreita análise sobre o processo de anonimização, ela não é capaz de, em si mesma, se legitimar como uma atividade de tratamento originalmente ilícita por inexistir fundamento legal para isso, esbarrando assim no princípio da finalidade.

Em outras palavras, se todo o processamento de dados precisa ser autorizado por uma norma que lhe dê suporte, a anonimização é um processo lícito, pois não é possível transformar uma atividade ilegal em legítima sem uma base legal. Dessa forma, o tratamento de dados pessoais deve ser realizado de acordo com objetivos legítimos, explícitos, específicos e informados ao titular quando da operação de dados pessoais[63].

Para uma melhor compreensão, imaginamos uma situação em que um dado é coletado e tratado sem uma hipótese legal que lhe permita assim realizar. Dessa forma, não será por meio da anonimização de dados que será removida a ilicitude do tratamento, devendo encerrar-se o mesmo e os dados serem eliminados.

---

[61] MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD Lei Geral de Proteção de Dados Comentada**. 2019. Revista dos Tribunais. 2. ed.

[62] A concepção da anonimização como processo tem sido adotada por várias autoridades de proteção de dados, havendo aquelas com estudos já publicados sobre o tema. Para referência, vide: Agência Espanhola de Proteção de Dados. Orientações e garantias nos procedimentos de anonimização de dados pessoais, 2016. p. 5. Disponível em: https://datos.gob.es/es/documentacion/orientaciones-y-garantias-en-los-procedimientos-de-anonimizacion-de-datos-personales

[63] Artigo 6º, inciso I, LGPD.

Assim, quando da coleta dos dados, é primordial que o controlador informe as finalidades, destacando-se que uma delas é a futura anonimização, de modo que se não houver informação prévia a sua realização importará tratamento posterior ou uso secundário, os quais devem ser compatíveis com a finalidade prévia informada aos titulares.

Deve a anonimização, como tratamento posterior, observar o princípio da adequação, que, por sua vez, determina que a licitude da operação de tratamento depende da sua compatibilidade com a(s) finalidade(s) legítima(s), específica(s) e explicitamente informada(s) ao titular dos dados, levando-se em consideração o contexto em que se realiza o tratamento[64].

Na tradição do direito de proteção de dados da União Europeia (UE), as noções de “adequação” e “uso compatível” são compreendidas como elementos estruturantes do princípio da finalidade ou da limitação dos propósitos (*purpose limitation principle*) de diversas normativas.

O princípio da necessidade é outra norma de alta relevância para a anonimização de dados. Conforme o art. 6º, III, o tratamento de dados pessoais deverá ser limitado ao mínimo necessário para a realização de suas finalidades, abrangendo apenas os “dados pertinentes, proporcionais e não excessivos em relação às finalidades” especificadas.

Em resumo, conforme demonstrado pelos princípios sobre tratamento de dados, “a anonimização não é uma medida de segurança impositiva, que deve ser adotada em todo e qualquer tratamento de dados pessoais”[65]. A pertinência da adoção do processo de anonimização decorre de um juízo de necessidade à luz das finalidades especificadas para o tratamento de dados na situação concreta.

De acordo com estudos recentes, é consenso que não há cenário em que não exista o risco de reidentificação dos dados anonimizados, devido ao elevado desenvolvimento da capacidade de processamento e análise de algoritmos de reidentificação. Sendo assim, deve-se adotar um modelo de anonimização baseado

---

[64] Artigo 6º, inciso II, LGPD.

[65] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo – Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Brasília: ANPD, 2023. p. 41; AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Nota Técnica nº 46/2022/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000730_2022_53-nt-46.pdf.

em riscos relacionados à identificabilidade de dados, de forma que este seja atualizado de forma constante, tendo em vista que novos riscos podem surgir com o avanço tecnológico e a quantidade de dados auxiliares disponíveis.

Conforme expresso no Estudo Preliminar sobre anonimização e pseudonimização, os riscos de reidentificação de dados anonimizados são expressos, em linguagem técnica, como possíveis ataques de reidentificação. O termo “ataque” é tomado por empréstimo da literatura especializada em segurança computacional, em que a avaliação do nível de segurança de determinado sistema computacional ou algoritmo de cifragem ocorre a partir do uso da figura de um hipotético “atacante” que possui certas habilidades, conhecimento ou acesso. “Uma avaliação de risco envolve a catalogação da variedade de potenciais atacantes e, para cada um, a probabilidade de sucesso”.

Cumpre ressaltar que essa noção de “atacante” não se confunde com aqueles sujeitos que praticam crimes ou atos antijurídicos. Basta considerar o exemplo de pesquisadores que avaliam a robustez de base de dados anonimizada compartilhada publicamente frente a certos algoritmos de reidentificação com o uso de dados auxiliares disponibilizados em bases de acesso público[66].

A figura do “atacante” muito se aproxima do “intruso” (*intruder*) a que a autoridade de proteção de dados da Irlanda se refere[67].

Sobre os riscos de reidentificação ou exemplos de ataques, podem ser mencionados a distinção, a possibilidade de ligação e a inferência. A distinção consiste na possibilidade de se isolar alguns ou todos os registros que destacam um indivíduo numa base de dados. A possibilidade de ligação é definida pela capacidade de se estabelecer uma conexão entre pelo menos dois registros relativos ao mesmo indivíduo ou ao mesmo grupo de pessoas. Já o risco de inferência diz respeito à possibilidade de inferir, com uma significativa probabilidade, o valor de um atributo a partir dos valores de um conjunto de outros atributos.

Para tanto, dois termos constantes na LGPD, em seu artigo 12, merecem destaque, sendo eles “esforços razoáveis” e “meios próprios”. O primeiro

---

[66] GARFINKEL, Simson L. **De-Identification of Personal Information**. [S.l.]: National Institute of Standards and Technology, 2015. p. 9.

[67] COMISSÃO DE PROTEÇÃO DE DADOS. **Guia sobre Anonimização e Pseudonimização.** [S.l.]: DPC, 2019. p. 8-10. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf

configura um conceito jurídico indeterminado normativo, ou seja, um conceito em larga medida incerto em seu conteúdo e extensão, dependente de preenchimento valorativo pelo aplicador do Direito.

Em termos práticos, isso significa que a ANPD, como intérprete e aplicadora da LGPD, deve preencher, com elementos e critérios pertinentes com o caso concreto, a noção de “esforços razoáveis”, no sentido literal possível e em coesão com o contexto significativo da lei, que, aliás, prevê no §1º do art. 12, relevantes parâmetros interpretativos.

Diferentemente da noção de “esforços razoáveis”, o conceito de meios próprios tem conteúdo mais delimitado, podendo-se afirmar que são meios próprios as habilidades, os dados, instrumentos e técnicas disponíveis ao próprio agente de tratamento responsável pela anonimização.

Sendo assim, importa ressaltar que, a partir do texto normativo do art. 12, caput, da LGPD, compreende-se que a avaliação da possibilidade de reidentificação de dados e a reversão do processo de anonimização devem ter em consideração não apenas o uso de meios próprios do agente de tratamento responsável pela anonimização, mas também a atuação de outras pessoas ou entidades que, com meios e esforços razoáveis, podem reidentificar conjunto de dados anonimizados.

Neste sentido, Carvalho e Canedo[68] apresentaram um conjunto com as melhores práticas de governança de dados. Os autores abordaram quatro desafios da anonimização de dados. Os desafios apresentados foram, primeiramente, que a informação ainda pode ser considerada pessoal mesmo quando o nome não está associado diretamente aos demais dados. Isso decorre do fato que a associação pode ocorrer através de outros dados.

Um segundo desafio é que a possibilidade de associação em bancos de dados com grandes volumes é alta quando as técnicas de anonimização utilizadas são mais simples, como o mascaramento por exemplo. Um terceiro desafio é referente a classificação do tipo de dado a ser anonimizado, a correta classificação desse dado

[68] CARVALHO, A. P.; CANEDO, E. D.; CARVALHO, F. P.; CARVALHO, P. H. P. Anonymisation and compliance to protection data: Impacts and challenges into big data. In: FILIPE, J.; SMIALEK, M.; BRODSKY, A.; HAMMOUDI, S. (Ed.). Proceedings of the 22nd International Conference on Enterprise Information Systems, ICEIS 2020, Prague, Czech Republic, May 5-7, 2020, Volume 1. SCITEPRESS, 2020. p. 31–41. Disponível em: https://doi.org/10.5220/0009411100310041.

como sendo um dado pessoal que pode ser utilizado como identificador é importante para evitar a reidentificação dessa informação.

E, ainda, como um quarto desafio tem a preocupação a respeito da dificuldade de determinar se um dado parcialmente anonimizado possa ser reidentificado por um critério adicional que possa surgir posteriormente por uma mudança técnica de tecnologia ou por uma decisão legal. Dessa maneira, esses desafios se referem à possibilidade de associação da informação anonimizada com seu significado real em um contexto de big data. Nesse cenário, considerando o maior volume de informações (big data), aumenta a possibilidade de uma reidentificação do dado[69].

5.2 PSEUDONIMIZAÇÃO

A pseudonimização não é equivalente à anonimização, uma vez que as informações ainda mantêm sua característica de dados pessoais. Esta significa substituir quaisquer características identificáveis dos dados por um pseudônimo, ou seja, um valor que não permite a identificação direta do titular dos dados.

A LGPD define a pseudonimização como o tratamento de dados pessoais de forma que esses dados não possam mais ser atribuídos a um titular de dados específico sem o uso de informações adicionais, desde que essas informações adicionais sejam mantidas separadamente; e estejam sujeitas a medidas técnicas e organizacionais para garantir que os dados pessoais não sejam atribuídos a um indivíduo identificado ou identificável[70].

Ao se utilizar um pseudônimo, a depender da técnica, é possível identificar o titular por meio da análise dos dados subjacentes ou relacionados, o que deve ser tratado com atenção à luz dos princípios da LGPD, a qual inclusive não indica técnicas específicas para tanto, apenas estabelecendo os referidos princípios e requisitos gerais.

Conforme o Estudo Preliminar, existem algumas técnicas de pseudonimização em conformidade com a LGPD, estando entre elas a substituição

---

[69] Op. Cit.

[70] ANPD. **ESTUDO PRELIMINAR. Anonimização e Pseudonimização para a proteção de dados pessoais.** 2023. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/37060

de dados, na qual dados pessoais são substituídos por pseudônimos ou códigos, tornando-os menos identificáveis. Por exemplo, um número de CPF pode ser substituído por um código alfanumérico único.

Enquanto a pseudonimização permite reidentificar e recuperar os dados originais, a anonimização, em tese, não. Neste contexto, uma das técnicas de anonimização seria a denominada k-anonimato, que busca garantir que a informação para cada pessoa seja indistinguível de pelo menos k − 1 outros indivíduos, cujas informações estejam nos dados disponibilizados, enquanto um método de pseudonimização seria a Tokenização, que consiste na substituição de dados por informações aleatórias denominadas como tokens[71].

Outras técnicas elencadas são a ofuscação de dados, a Tokenização, a cifração, o mascaramento de dados e o Salting. Com relação à ofuscação de dados, envolve a transformação de dados pessoais de forma que sejam mais difíceis de identificar. Isso pode incluir o embaralhamento de informações ou a substituição de valores de dados por outros valores semelhantes.

A Tokenização envolve a substituição de dados pessoais por tokens ou códigos que não têm significado fora do contexto do sistema. Esses tokens podem ser usados para fins de identificação, mas não revelam as informações reais dos titulares de dados.

A cifração, por sua vez, é a técnica que converte dados em um formato criptografado que só pode ser decifrado com uma chave. Isso torna os dados pessoais ilegíveis para qualquer pessoa sem acesso à chave correspondente.

O mascaramento de dados envolve a ocultação parcial de informações, revelando apenas uma parte dos dados e ocultando o restante. Por exemplo, um número de telefone pode ser mascarado como "(XX) XXXX-1234", mostrando apenas os últimos dígitos.

E por fim, Salting é a técnica comumente utilizada na criptografia de senhas. Um valor aleatório (chamado de "salt") é adicionado aos dados antes da encriptação, tornando os pseudônimos únicos e mais seguros contra-ataques de força

---

[71] SOUSA, Thiago do Rego; COUTINHO, Murilo; COUTINHO, Lilian; ALBUQUERQUE, Robson. **LGPD: Levantamento de Técnicas Criptográficas e de Anonimização para Proteção de Bases de Dados**. Sociedade Brasileira de Computação (SBC). 2020. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/19227/19056.

bruta[72].

O documento destaca que Criptografia típica não é anonimização, mas sim uma técnica de pseudonimização. Como a informação original precisa estar acessível, as transformações aplicadas pelos algoritmos criptográficos são projetadas para serem reversíveis, no que é conhecido como descriptografia. Entretanto, vários algoritmos criptográficos (simétricos, assimétricos e de hash) podem realizar processamentos unidirecionais. Nesses casos, atendem-se os requisitos da anonimização, desde que os dados cifrados sejam úteis.

A criptografia envolve a codificação de informações compreensíveis por meio de algoritmos, que transformam um texto inicial em um conteúdo totalmente ilegível. É viável realizar o processo oposto, a descriptografia, para recuperar essas informações[73].

Em um sistema criptográfico é necessário que tanto o remetente quanto o destinatário empreguem o mesmo sistema. Uma qualidade fundamental de um sistema criptográfico eficaz é que o algoritmo em si seja de conhecimento público. De maneira geral, existem três categorias de algoritmos criptográficos: criptografia simétrica, assimétrica e unidirecional.

No sistema simétrico, o remetente e o destinatário compartilham um algoritmo e uma chave secreta. Por isso, se faz essencial que tal chave seja protegida e que seja trocada sempre antes da comunicação entre remetente e destinatário, pois é utilizada por ambos. Quanto maior o número de remetentes/destinatários trocando as mensagens, maior o risco de comprometimento da chave, uma vez que pode ser interceptada por um agente ameaçador, principalmente se ela não estiver adequadamente protegida[74].

Segundo o National Institute of Standards and Technology (NIST)[75], que é uma agência governamental não regulatória da administração de tecnologia do

---

[72] ANPD. **ESTUDO PRELIMINAR. Anonimização e Pseudonimização para a proteção de dados pessoais**. 2023. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/37060

[73] SILVA, Lucas Henrique de Moura e. **Escolha da Criptografia Ideal e Anonimação de Dados Sensíveis Citados a Lei Geral de Proteção de Dados**. 2020. Disponível em: http://45.4.96.19/bitstream/aee/17213/1/TCC2%20WiLucasHenrique_Final.pdf.

[74] HINTZBERGEN, Kees; HINTZBERGEN, Jule; BAARS, Hans. **Fundamentos de Segurança da Informação: com Base na ISO 27001 e na ISO 27002**. 1. ed. São Paulo: Brasport, 2018

[75] GREENBERG, C. S.; MASON, L. P.; SADJADI, S. O.; REYNOLDS, D. A. **Two decades of speaker recognition evaluation at the national institute of standards and technology**. Comput. Speech Lang., v. 60, 2020. Disponível em: https://doi.org/10.1016/j.csl.2019.101032.

Departamento de Comércio dos Estados Unidos, referência em padronizações associadas a Cibersegurança, o ciclo de vida de uma chave criptográfica é iniciado com a sua geração e somente finalizado com seu descarte e adequada eliminação. Durante este processo passa pela geração, pré-ativação, ativada, suspensa, inativada, comprometida ou destruída.

O gerenciamento de chaves criptográficas envolve, ainda, a realização de cópias de segurança, em razão da chave criptográfica ser o único instrumento que associado ao algoritmo criptográfico utilizado pode reverter a anonimização das informações, a ausência de cópias de segurança aumenta significativamente os riscos associados ao processo, com consequências possíveis de perda total de acesso a informação[76].

Para que a pseudonimização seja eficaz, as informações adicionais que permitem a reversão dela (por exemplo, as chaves criptográficas) devem ser mantidas separadamente e protegidas por medidas técnicas e organizacionais adequadas, mantendo-se, claramente, a privacidade e a segurança dos dados pessoais em todas as etapas do tratamento.

Para Lucas Henrique de Moura Silva, a LGPD dispõe que os dados anonimizados, em princípio, estão vinculados a uma pessoa, mas passaram por etapas que garantiram a sua desvinculação do usuário. Ensina ainda que os bancos de dados disponibilizam funções para propiciar a anonimização dos dados, impedindo a identificação do usuário através do dado tratado, e nos apresenta técnicas de anonimização dos dados, de acordo com PostgreSQL Anonymizer[77].

Do ponto de vista técnico, de maneira geral, a pseudonimização é atingida substituindo uma informação pessoal significativa que identifica o titular, o que resulta na perda da capacidade de associação direta ou indireta a um indivíduo. Essa associação só se torna possível com o uso de informações extras, mantidas de forma restrita pelo responsável pelo tratamento. Entretanto, essa simples modificação não é suficiente para impedir a identificação do titular dos dados, especialmente diante de eventual tentativa de "força bruta", que envolve

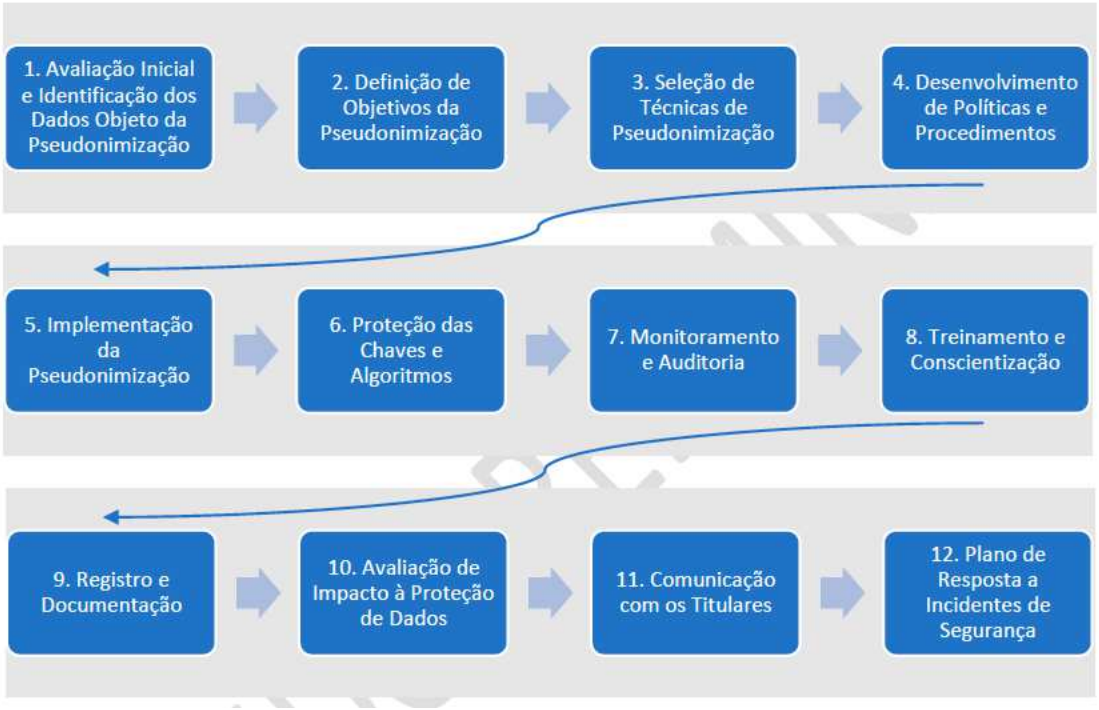
---

[76] BRAEKEN, A. **Public key versus symmetric key cryptography in client-server authentication protocols**. Int. J. Inf. Sec., v. 21, n. 1, p. 103–114, 2022. Disponível em: https://doi.org/10.1007/ s10207-021-00543-w.
[77] Op. Cit.

testar todas as possibilidades concebíveis para reidentificar o titular[78].

Sobre uma metodologia eficaz de pseudonimização, foi elaborado um esquema pelo Estudo Preliminar:

Figura 2: Esquema de pseudonimização



Fonte: Estudo preliminar, 2023[79].

Conforme ilustração acima, para o desenvolvimento dessa metodologia, algumas etapas devem ser observadas. A primeira etapa trata-se da "Avaliação Inicial e Identificação dos Dados Objeto da Pseudonimização", com uma avaliação abrangente de quais dadospessoais serão coletados e tratados. Deve ser identificado quais dados pessoais serão objeto da pseudonimização, considerando os riscos e o tratamento realizado, dando ênfase a dados considerados sensíveis como, por exemplo, dados de saúde, origem racial ou étnica, convicção religiosa, opinião política, entre outros.

---

[78] MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD Lei Geral de Proteção de Dados Comentada**. 2019. Revista dos Tribunais. 2. ed.

[79] ANPD. **ESTUDO PRELIMINAR. Anonimização e Pseudonimização para a proteção de dados pessoais**. 2023. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/37060

Após, é realizada a definição de “Objetivos da Pseudonimização”, estabelecendo claramente os objetivos da pseudonimização, incluindo a proteção da privacidade do titular dos dados, a redução do risco de violações de dados e o cumprimento da LGPD. Também é realizada a seleção de Técnicas de Pseudonimização, escolhendo as técnicas de pseudonimização apropriadas com base na natureza dos dados.

A ANPD realizou uma consulta pública à sociedade sobre o estudo preliminar da anonimização e pseudonimização, com início em 30 de janeiro de 2024 e término em 14 de março de 2024. O objetivo era receber contribuições de profissionais da área, dos agentes de tratamento, dos titulares, do setor acadêmico e da sociedade em geral, de forma a permitir uma atuação regulatória adequada às melhores práticas e à realidade[80].

Isto comprova que ainda se tratam de padrões em desenvolvimento, onde provavelmente muito em breve irá possuir regulamentação própria, complementar a LGPD, a fim de servir de base para os agentes de tratamento quando da realização de ambos os procedimentos, no cumprimento de suas atribuições e em respeito aos princípios da LGPD para o melhor tratamento.

Neste sentido, passa-se à análise de como ocorre a atuação do operador de dados perante os processos de anonimização e pseudonimização, utilizando-os principalmente como medidas de segurança para diminuir os riscos de ocorrência de incidentes de segurança.

[80] ANPD. **ESTUDO PRELIMINAR. Anonimização e Pseudonimização para a proteção de dados pessoais**. 2023. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/37060

6 A ATUAÇÃO DO OPERADOR EM RELAÇÃO À ANONIMIZAÇÃO E À PSEUDONIMIZAÇÃO COMO MEDIDAS DE SEGURANÇA

O art. 46 da Lei dispõem que os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

Assim, é dever do controlador e do operador dos dados adotar medidas a fim de que os dados pessoais utilizados sejam protegidos. Essa obrigação ainda ganha uma ampliação e atinge até mesmo as pessoas que intervirem, de alguma forma, no processo de tratamento dos dados.

Como já visto, os processos de anonimização e pseudonimização são utilizados para fins específicos, a exemplo de censos escolares e dados relativos à saúde, mas também podem ser utilizados como uma ferramenta, uma medida de segurança quando do simples tratamento dos dados pessoais pelos agentes de tratamento. Realizando o tratamento em nome do controlador, e nos limites por ele estabelecidos, o operador tem atuação ativa na realização de tais processos.

Um elemento indispensável para se caracterizar um sujeito como operador é a realização efetiva de operações de tratamento de dados pessoais. Como se sabe, o tratamento abrange uma coleção de operações com dados pessoais, consoante o art. 5º, inc. X, da LGPD: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, entre outras.

Destaca-se também que o operador deve ser entidade autônoma e só pode promover operações de tratamento de dados pessoais que estejam dentro do perímetro e das finalidades definidas pelo controlador. Assim, o operador não pode realizar o tratamento para as suas próprias finalidades, podendo inclusive ser responsabilizado caso vá além das orientações do controlador.

Neste cenário, revelam-se as obrigações mais visíveis do operador:

> (i) atuar em consonância com as instruções do controlador; (ii) celebrar contratos que estabeleçam, dentre outros assuntos, o regime de

> atividades e responsabilidades com o controlador; e (iii) dar ciência ao controlador em caso de contrato com suboperador[81].

Cappello sublinha que “é importante que a relação contratual entre o controlador e o operador contemple a observância das normas da LGPD e, também, as instruções detalhadas para o tratamento de dados pessoais”[82].

Para compreensão sobre a figura do operador, a ANPD menciona diversos exemplos. O exemplo 08 trata de e-commerce. Em um canal de vendas online de livros, que conta com diversas formas de pagamento, tem-se que o canal que realiza a venda é o controlador dos dados pessoais, enquanto cada serviço de pagamento disponível será um operador diferente. Por exemplo: a empresa de cartão de crédito, uma *fintech*, o banco em caso de transferências bancárias, dentre outros. O operador dessa transação, seja ele qual for, não poderá utilizar os dados fornecidos para novas finalidades que não aquelas determinadas pelo controlador.

O exemplo 09 trazido pela autoridade trata de call center. A empresa XRAY tem sob sua responsabilidade os dados de seus clientes e repassa para uma empresa terceirizada de call center, ZULU, que recebe as informações. A empresa XRAY é a controladora e o call center terceirizado ZULU, o operador, que executará o tratamento de dados dos clientes a mando da empresa XRAY. Caso realize o tratamento de dados fora do que foi orientado pelo controlador, a empresa ZULU poderá ser responsabilizada.

O exemplo 10 fala sobre os servidores públicos, onde uma autarquia, entidade da administração pública indireta, com personalidade jurídica própria, deseja utilizar um novo software para aprimorar o gerenciamento dos funcionários da instituição. Para isso, a Secretaria de Gestão Corporativa da entidade delega à Diretoria de Gestão de Pessoas (DGP) a tarefa de determinar os meios pelos quais este software será implementado. Após algumas reuniões, a DGP decide pela contratação da empresa terceirizada SIERRA para desenvolver o software em parceria com a equipe interna da Diretoria de Tecnologia da Informação (DTI).

---

[81] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.** Brasília: ANPD, 2021

[82] CAPPELLO, Thamires. “Dos agentes de tratamento de dados pessoais”. *In:* DANTAS, Eduardo *el al* (Coord.). **Comentários à Lei Geral de Proteção de Dados Sob a Perspectiva do Direito Médico e da Saúde.** Indaiatuba: Foco, 2023

Embora a delegação de decisão quanto aos meios para a DGP possa sugerir que essa diretoria atue como operadora de dados, esta não é a análise correta: como a DGP é uma unidade administrativa da autarquia, a delegação interna não altera o papel do agente de tratamento., uma vez que, como exposto, o operador será sempre pessoa distinta do controlador. O mesmo raciocínio se aplica para a DTI. Desse modo, a autarquia será a controladora de dados e a empresa SIERRA será a operadora de dados. A Secretaria e as Diretorias, assim como os seus respectivos servidores, são apenas unidades organizacionais do ente controlador de dados, razão pela qual não se caracterizam como agentes de tratamento[83].

Para haver uma proteção eficiente, em seu capítulo VIII, a lei estabeleceu algumas sanções para quem descumprir as obrigações impostas. A RESOLUÇÃO CD/ANPD Nº 4, DE 24 DE FEVEREIRO DE 2023, aprovou o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Em seu anexo, são estabelecidos parâmetros e critérios para aplicação de sanções administrativas pela Autoridade Nacional de Proteção de Dados (ANPD), bem como as formas e dosimetrias para o cálculo do valor-base das sanções de multa.

Algumas definições são trazidas para servirem como base para a aplicação das sanções. O infrator é definido como o agente de tratamento que compete à infração. Infração, por sua vez, é definida como o descumprimento de obrigação estabelecida na Lei nº 13.709, de 14 de agosto de2018 (LGPD), e nos regulamentos expedidos pela ANPD, diferenciando-se da infração permanente pelo fato de esta ser uma conduta infrativa que se prolonga no tempo, mediante ação ou omissão do infrator referente ao mesmo dispositivo normativo.

Medidas corretivas são definidas como as determinadas pela ANPD com a finalidade de corrigir a infração e reconduzir o infrator à plena conformidade à LGPD e aos regulamentos expedidos pela ANPD, devendo ser aplicadas conjuntamente com a sanção de advertência, nos termos do Regulamento.

A política de boas práticas e de governança se trata de normas e processos internos que assegurem o cumprimento abrangente da legislação de proteção de dados pessoais, estabelecidos e implementados pelo agente de

---

[83] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.** Brasília: ANPD, 2021

tratamento mediante a adoção de regras de boas práticas e de governança, nos termos do art. 50, caput e § 1º, da LGPD; ou programa de governança em privacidade, nos termos do § 2º do art. 50 da LGPD[84].

Superadas as definições, são apresentadas as sanções, as quais assim se dividem em advertência (nos termos do artigo 9º da resolução CD/ADNPD nº4); multa simples (artigo 10º do regulamento); multa diária (art. 16 do regulamento); publicização da infração, após devidamente apurada e confirmada a sua ocorrência (artigos 20 e 21); e bloqueio dos dados pessoais a que se refere a infração, até a sua regularização (art. 22).

Ainda se apresentam como sanções a eliminação dos dados pessoais a que se refira a infração (artigo 23); suspensão parcial do funcionamento do banco de dados a que se refira a infração (art. 24); suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração (art. 25); e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (art. 26)[85].

As infrações são classificadas conforme a sua gravidade e a natureza dos direitos pessoais afetados, subdividindo-se em leve, média ou grave. Para um melhor esclarecimento, ainda explica o que seria a definição de sanção, considerando os parâmetros e critérios dispostos no artigo 7º da Resolução CD/ANPD nº 4 de 2003.

Entre os critérios, encontram-se a gravidade e a natureza das infrações dos direitos pessoais afetados; a boa-fé do infrator; a vantagem auferida ou pretendida pelo infrator; a condição econômica do infrator; a reincidência específica e a genérica; o grau do dano; a cooperação do infrator; a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com a LGPD; a adoção de boas práticas e governança e de medidas corretivas; e a proporcionalidade entre a gravidade da falta e a intensidade da sanção[86].

Uma infração será considerada leve quando não for verificada nenhuma das situações que a enquadre como média ou grave. Ou seja, não se enquadrando nas definições das demais, será uma infração leve.

A infração será considerada média quando puder afetar

[84] Art. 2º, RESOLUÇÃO CD/ANPD Nº 4, DE 24 DE FEVEREIRO DE 2023.
[85] Art. 3º, RESOLUÇÃO CD/ANPD Nº 4, DE 24 DE FEVEREIRO DE 2023.
[86] Art. 7º, RESOLUÇÃO CD/ANPD Nº 4, DE 24 DE FEVEREIRO DE 2023.

significativamente interesses e direitos fundamentais dos titulares de dados pessoais, caracterizada nas situações em que a atividade de tratamento puder impedir ou limitar, de maneira significativa, o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação; violação à integridade física; ao direito à imagem e à reputação; fraudes financeiras ou uso indevido de identidade, desde que não seja classificada como grave, como disposto no parágrafo segundo do artigo oitavo.

Por fim, a infração será considerada grave quando, verificar-se cumulativamente uma infração média e envolver outras hipóteses como, por exemplo, o tratamento de dados pessoais em larga escala, caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.

Também será considerada grave quando somar uma infração média a uma situação em que o infrator auferir ou pretender auferir vantagem econômica em decorrência da infração cometida; realizar tratamento de dados pessoais sem amparo em uma das hipóteses legais previstas na LGPD; adotar sistematicamente práticas irregulares ou realizar tratamento com efeitos discriminatórios ilícitos ou abusivos.

Se a infração envolver tratamento de dados sensíveis ou de dados pessoais de crianças, de adolescentes, de idosos ou implicar risco à vida dos titulares ou envolver o tratamento de dados sensíveis ou de dados pessoais de crianças, de adolescentes ou de idosos, também poderá somar-se a infração média e ser considerada grave. Por fim, não poderá a atuação do infrator constituir obstrução à atividade de fiscalização[87].

Ainda sobre o grau do dano, há uma figura onde se dispõe de uma tabela relacionando os valores:

[87] Art. 8º, §3º, RESOLUÇÃO CD/ANPD Nº 4, DE 24 DE FEVEREIRO DE 2023

Figura 3: Tabela de valores para grau do dano

Valor	Grau do Dano
3	A infração ocasiona lesão ou ofensa a direitos ou interesses difusos, coletivos ou individuais, que, dadas as circunstâncias extraordinárias do caso, têm impacto irreversível ou de difícil reversão sobre os titulares afetados, de ordem material ou moral, ocasionando, entre outras situações, discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou uso indevido de identidade; ou Danos decorrentes de litigância de má-fé, tais como, entre outras hipóteses previstas na legislação processual, alteração da verdade dos fatos, uso do processo para conseguir objetivo ilegal, resistência injustificada ao andamento do processo, atuação temerária em qualquer ato do processo ou impedimento da atuação da ANPD.
2	A infração ocasiona lesão ou ofensa a direitos ou interesses difusos, coletivos ou individuais, que, dadas as circunstâncias do caso, geram impactos aos titulares, de ordem material ou moral, que não se enquadram nos critérios indicados na descrição do grau de dano 0, 1 ou 3; ou Dano decorrente do envio de informações intempestivas ou cumprimento intempestivo com prejuízo direto para o processo de fiscalização ou administrativo sancionador ou para terceiros e que não decorra de litigância de má-fé.
1	A infração ocasiona lesão ou ofensa a direitos ou interesses de um número reduzido de titulares, com impacto de ordem material ou moral limitado, que pode ser revertido ou compensado com relativa facilidade; ou Descumprimento de determinação ou envio ou disponibilização de informações fora dos prazos ou condições estabelecidos pela ANPD, sem prejuízo direto para o processo de fiscalização ou administrativo sancionador ou para terceiros e que não decorra de litigância de má-fé.
0	A infração não ocasiona danos ou somente ocasiona danos com impactos insignificantes aos titulares, que decorrem de situações previsíveis ou corriqueiras e que não justificam a necessidade de compensação.

Fonte: RESOLUÇÃO CD/ANPD Nº 4, DE 24 DE FEVEREIRO DE 2023

De forma geral, é possível destacar que o regulador, ao prever as sanções na LGPD, o fez a partir de uma concepção de escalonamento, que ocorre de acordo com as características do caso concreto e que toma em consideração as medidas de conformidade adotada pelos agentes de tratamento.

As sanções serão aplicadas após procedimento administrativo mediante decisão fundamentada da ANPD, assegurado o direito à ampla defesa, ao contraditório e ao devido processo legal, não excluindo ainda a possibilidade de adoção de outras medidas administrativas pela ANPD, previstas na LGPD e no Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador.

Nota-se que o operador tem o dever de implementar medidas técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais, podendo responder em casos de incidentes de vazamento de dados, inclusive nas sanções acima apresentadas.

Sobre o tema, a responsabilidade civil está disposta na Seção III do Capítulo VI da referida lei. Ali também está expresso sobre o ressarcimento dos danos. O artigo 42 é de suma importância para o tema, além dos artigos seguintes. O artigo 46 estabelece, por exemplo, que todos os agentes de tratamento devem adotar medidas de segurança, sempre visando à proteção dos dados pessoais dos usuários.

Nesta seara, existem correntes doutrinárias divergentes sobre a responsabilidade civil ser subjetiva ou objetiva. Analisando-se a questão da responsabilidade de modo superficial, visto não ser o enfoque principal do estudo, destaca-se que a corrente que afirma que a responsabilidade do agente de tratamento pelo evento danoso (vazamento de dados, incidentes de segurança, etc.) é objetiva uma vez que se assume o risco da atividade, ou até mesmo adotando-se o risco integral (onde não seria possível aplicar excludentes de responsabilidade civil), deixando de lado a intenção do agente. Ao contrário, a corrente que adota a responsabilidade subjetiva afirma que é preciso analisar a culpa do agente diante das obrigações impostas em lei.

A LGPD já prevê hipóteses de mitigação da responsabilidade do operador de dados compatíveis com a situação daqueles sujeitos a uma força diretiva externa que limite o seu poder de decisão, inclusive em relação ao subordinado no cumprimento de regras impostas pelo controlador-empregador.

Por exemplo, o artigo 39 prevê que o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará, por sua vez, o cumprimento dessas regras e da licitude das ações dos que agem em seu nome.

Igualmente, no artigo 42, ao fixar as responsabilidades do controlador e do operador no exercício de atividade de tratamento de dados pessoais, é assegurado no inciso I do §1º do dispositivo a mitigação dessa responsabilidade do operador, a qual limitada a hipótese de danos causados pelo tratamento em descumprimento às obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador.

Se o operador tomar conhecimento de um incidente de segurança envolvendo dados pessoais, deverá notificar o controlador sem atrasos injustificados. O operador também deve colaborar com o controlador para que este mitigue os riscos causados em relação a violações de dados pessoais, notificando-o imediatamente caso alguma das suas instruções leve a uma violação da LGPD ou demais leis aplicáveis.

Muito se fala sobre a responsabilidade civil quando da ocorrência de incidentes, mas pouco se discute sobre a atuação durante o tratamento para que

ocorra dentro dos parâmetros previstos no ordenamento, e como forma de prevenção a vazamentos de dados.

Assim, cumpre então o estudo de como se dá a atuação dos agentes de tratamento no processo de tratamento de dados, em especial quanto ao operador de dados, a fim de compreender seu papel também nos processos de anonimização e pseudonimização e como prevenção da ocorrência de incidentes de segurança neste processo.

Conforme disposto no guia de proteção de dados para pequenos negócios do GDPR[88], a segurança dos dados tem três componentes principais: proteger a integridade, disponibilidade e confidencialidade dos dados. Portanto, as organizações devem avaliar os riscos para acesso não autorizado ou acidental aos dados (violação da confidencialidade), alteração não autorizada ou acidental de dados (violação da integridade) e perda de dados ou perda de acesso aos dados (violação da disponibilidade).

É igualmente aconselhável identificar as fontes de risco (ou seja, quem ou o que pode estar na origem de cada incidente de segurança), tendo em conta fontes humanas internas e externas, como por exemplo o administrador informático, utilizador, atacante externo, concorrente etc.; e fontes não humanas internas ou externas, como por exemplo danos causados por água, materiais perigosos, vírus informáticos não visados, entre outros.

Também no GDPR se fala acerca de anonimização e pseudonimização de dados, sendo a pseudonimização uma das medidas recomendadas pelo RGPD para limitar os riscos associados ao tratamento de dados pessoais, além da criptografia e da anonimização.

As autoridades europeias de proteção de dados definem três critérios para garantir que um conjunto de dados é verdadeiramente anónimo: Individualização: não deve ser possível isolar informações sobre um indivíduo no conjunto de dados; Correlação: não deve ser possível ligar elementos de dados separados relativos ao mesmo indivíduo; e Inferência: não deve ser possível deduzir, com quase certeza, informações sobre um indivíduo[89].

---

[88] EDPB. **Dados pessoais seguros.** Disponível em: https://www.edpb.europa.eu/sme-data-protection-guide/secure-personal-data_pt

[89] Op. Cit.

Do estudo se percebe que na União Europeia também encontram-se dificuldades no que se trata de pseudonimização e anonimização de dados, em especial quanto a anonimização, visto que na prática lá também nem sempre é possível alcançar, devendo-se avaliar se a anonimização pode ser aplicada aos dados em causa e mantida com êxito, tendo em conta as circunstâncias específicas do tratamento dos dados pessoais, sendo necessário ainda, por vezes, conhecimentos jurídicos ou técnicos adicionais para concretizar com êxito a anonimização em conformidade com o GDPR[90].

Ainda sobre o tema anonimização, os dados que tenham sido tornados irreversivelmente anonimizados deixam de ser considerados "dados pessoais" e o processamento desses dados não exige conformidade com a legislação de proteção de dados. Isso implica que as organizações podem utilizá-los para finalidades, desde que compatíveis, que vão além daquelas para as quais foram originalmente coletados e esses dados podem ser mantidos indefinidamente.

O processo de anonimização, orientado por uma abordagem baseada em riscos, tem como objetivo fornecer um conjunto mínimo de etapas que podem servir de guia de boas práticas aos agentes de tratamentos de dados. Essas etapas sugerem que o agente identifique e compreenda os riscos envolvidos em sua atividade, bem como adote medidas para mitigá-los.

A abordagem da anonimização como um processo contínuo baseado em risco possibilita que o agente de tratamento defina, de acordo com seu contexto, o compromisso entre o grau de utilidade e o grau de anonimização que contemple a finalidade definida no tratamento e minimize o risco de reidentificação do titular. Importante ressaltar que os processos de anonimização e pseudonimização encontram vinculação tanto no direito quanto na tecnologia da informação, sendo impossível dissociá-los, de forma que sua análise é sempre apresentada em conjunto.

A discussão do processo de anonimização é iniciada com a apresentação do conflito entre a utilidade e o grau de anonimização do dado pessoal, seguida por uma importante ponderação sobre a gestão do risco de reidentificação de dados anonimizados por meio de um processo de anonimização baseado em risco.

Não há técnica de anonimização com eficácia plena, tendo todas elas

---

[90] Op. Cit.

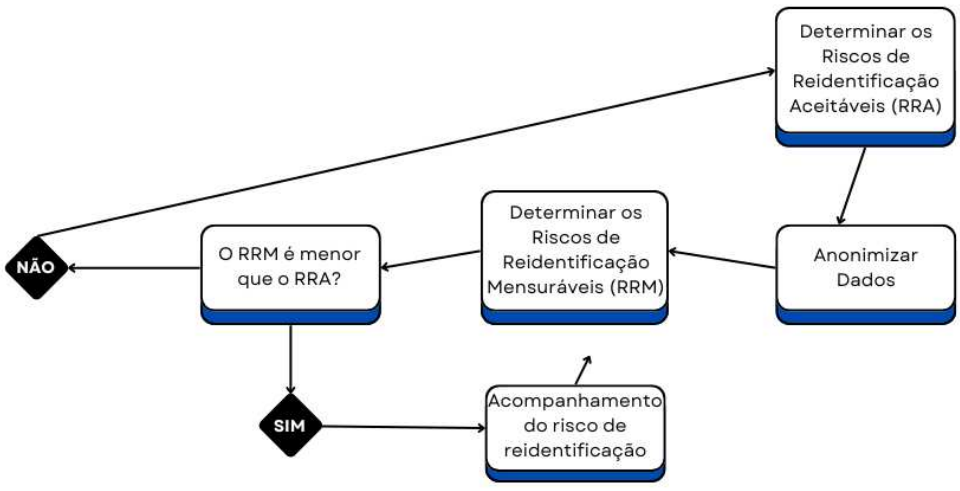
um risco de reidentificação associado, cabendo ao agente de tratamento gerenciar esse risco com a adoção de um processo de anonimização adequado. Para isso, a gestão do risco de reidentificação deve ser realizada de forma contínua durante todo o tratamento dos dados, permitindo que o agente de tratamento tenha evidências suficientes para a tomada de decisão relacionada à proteção de dados e à privacidade dos titulares.

Gunawan e Mambo exploraram a anonimização de dados através do método de substituição, e os resultados experimentais mostraram que o método proposto reduziu com sucesso a probabilidade de sucesso de ataque em um banco de dados anonimizado minimizando a perda de informações[91].

O cenário de anonimização apresenta características que podem variar para a realidade de cada agente de tratamento. Por esse motivo, a anonimização não deve se restringir à discussão de técnicas, mas sim uma abordagem mais ampla baseada em processo.

Sobre o processo, há indicação de uma sequência por meio do estudo preliminar, sobre o qual se apresenta a figura abaixo:

Figura 4: Processo de anonimização dos dados



Fonte: A autora

[91] GUNAWAN, D.; MAMBO, M. **Data anonymization for hiding personal tendency in set- valued database publication.** Future Internet, v. 11, n. 6, p. 138, 2019. Disponível em: https: //doi.org/10.3390/fi11060138.

O Risco de Reidentificação Mensurado (RRM) deve ser comparado ao Risco de Reidentificação Aceitável (RRA). Caso o RRM seja maior do que o RRA, o conjunto de dados não apresenta a condição de estar anonimizado, sendo necessário o reinício do processo de anonimização. Caso contrário, é necessário acompanhar o uso do conjunto de dados, especialmente quando operações realizadas sobre ele possam modificar o risco mensurado, tais como operações de inclusão, alteração ou deleção de dados; havendo essas operações, é necessário atualizar o nível do risco mensurado.

A primeira etapa consiste na determinação do Risco de Reidentificação Aceitável (RRA) para um certo conjunto de dados, e visa estipular um limite superior para o risco. Um risco de reidentificação superior ao limite estabelecido descaracterizará o conjunto de dados como anonimizado. Pode-se citar como exemplos de variáveis de contexto a existência de dados pessoais sensíveis ou dados financeiros que podem diminuir o limite do risco aceitável.

A segunda etapa consiste na aplicação do conjunto de técnicas de anonimização escolhido. O objetivo dessa etapa é produzir um conjunto de dados anonimizados que tenha um risco de reidentificação não superior ao limite do risco aceitável definido na etapa anterior. A escolha das técnicas de anonimização deve considerar as características dos dados.

A terceira etapa consiste em definir o Risco de Reidentificação Mensurado (RRM) de um ataque de reidentificação ter sucesso no conjunto de dados, pós-anonimização. De modo semelhante à primeira etapa, variáveis dependentes do contexto podem ser observadas pelo agente de tratamento, como exemplo, tem-se a condição do conjunto de dados ser público, compartilhado ou privado. Essa condição pode afetar o risco real de reidentificação.

Para dados textuais estruturados, há algumas métricas de mensuração de risco bem conhecidas na área de TI, tais como a K-Anonimização[92], T-Proximidade[93] e L-Diversidade[94]. Essas métricas derivam de uma métrica base que

[92] SAMARATI, P.; SWEENEY. L. **Protecting privacy when disclosing information: k-anonymity and tis enforcement through generalization and suppression**. Technical Report, 1998

[93] LI N.; LI, T.; VENKATASUBRAMANIAN S. **T-Closeness: Privacy Beyond k-Anonymity and L-Diversity**. IEEE 23rd International Conference on Data Engineering, 2007.

[94] AGGARWAL, Charu C.; YU, Philip S. **A general Survey of Privacy-Preserving Data Mining Models and Algorithms**. Privacy-Preserving Data Mining. Advances in Database System. vol 34. Springer. 2008.

utiliza o conceito de equivalência de classe da teoria dos conjuntos para determinar o risco de reidentificação.

Do ponto de vista tecnológico, a implementação eficaz da anonimização e pseudonimização depende da adoção de uma série de controles de segurança, como: controle de acesso, para garantir que apenas indivíduos autorizados possam acessar dados pessoais; criptografia de ponta a ponta, protegendo os dados enquanto estão em trânsito e enquanto são armazenados; monitoramento e auditoria contínuos, verificando o uso e acesso aos dados em tempo real, para prevenir possíveis brechas de segurança; e segregação de dados, com o armazenando os dados em locais físicos ou lógicos separados, a fim de minimizar riscos em caso de comprometimento.

A dúvida que surge durante todo esse processo é qual seria a importância ou relevância dele, uma vez que se trata de um processo complexo. Sobre a sua finalidade, pode ser amplamente utilizado, a exemplo de dados de saúde coletados, pesquisas acadêmicas, dados de sensos, entre outros.

No que se refere aos atendimentos em saúde, é inquestionável que o profissional da saúde deve registrar o tratamento realizado a cada paciente por meio do prontuário médico. Logo, tais dados são necessários tanto ao paciente que necessita ser devidamente informado sobre o procedimento hospitalar adotado, tanto ás próprias instituições de saúde.

Sobre os dados relativos a estudos e pesquisas, foi emitida a Nota Técnica nº 46/2022/CGF/ANPD com o assunto “Adequação dos microdados disponibilizados para o atendimento às exigências previstas na Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD)”, cujo interessado é o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP).

Sobre a nota, destaca-se que tem por fundamento a suspensão da divulgação dos microdados do censo escolar e do Exame Nacional do Ensino Médio (Enem) pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) e a posterior publicação da NOTA de Esclarecimento INEP (SEI nº 3289150) no sítio eletrônico do instituto, na qual a Autarquia federal esclarece que a adequação dos microdados disponíveis em seu portal está sendo realizada com base em estudos

técnicos e análises jurídicas que priorizem o pleno atendimento às exigências previstas na Lei nº 13.709, de 14/08/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD).

A necessidade de adequação das divulgações se dá em observação a critérios objetivos que reduzam o risco potencial de identificação das pessoas a quem os dados estatísticos se referem, e tem por base estudo realizado em parceria com a Universidade Federal de Minas Gerais (UFMG) por meio de Termo de Execução Descentralizada (TED 8750, SEI nº 3289230) e executado pelo Laboratório Inscrypt (Laboratory of Information Security, Cryptography, Privacy, and Transparency) do Departamento de Ciência da Computação (DCC) da universidade.

No referido estudo, foi constatado que as técnicas de proteção de privacidade utilizadas nos microdados para retirada de identificadores individuais, como nome e número do Cadastro de Pessoas Físicas (CPF) e do Registro Civil, estão sujeitas a riscos já identificados. Nele, consta a conclusão de que a atual forma de divulgação dos censos educacionais pelo INEP submete os titulares dos dados a consideráveis riscos de violação de privacidade, incluindo reidentificação e inferência de atributos sensíveis, circunstância que poderia constituir violação à LGPD[95].

Do exposto, retira-se a importância da anonimização dos dados coletados referentes à divulgação dos microdados do censo escolar e do Exame Nacional do Ensino Médio (Enem).

Consta na nota, inclusive, o item III, intitulado “ANONIMIZAÇÃO, DIVULGAÇÃO PÚBLICA DE DADOS PESSOAIS E ELABORAÇÃO DE RELATÓRIO DE IMPACTO”, onde consta que, em resumo, os dados anonimizados não são considerados dados pessoais, por isso não estão sujeitos às disposições da LGPD, salvo quando o processo de anonimização a que foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido (art. 12).

A determinação do que seja esforço razoável deve considerar fatores objetivos, tais como o custo e o tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis no momento da

[95] ANPD. **Nota Técnica nº 46/2022/CGF/ANPD**. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000730_2022_53-nt-46.pdf.

anonimização, e a utilização exclusiva de recursos tecnológicos próprios do agente de tratamento (art. 12, § 1º).

Importante destacar que a anonimização não é uma medida de segurança impositiva, que deve ser adotada em todo e qualquer tratamento de dados pessoais. De forma mais específica, a LGPD não estabeleceu a anonimização como condição técnica para a divulgação pública ou para o compartilhamento de dados pessoais por entidades e órgãos públicos.

Ao contrário, como já mencionado, a principal determinação da LGPD é quanto à necessidade de avaliação de riscos e de adoção de medidas para mitigar a ocorrência de danos. Por isso, a eventual identificação dos titulares ou a admissão de algum grau de risco de sua identificação, quando necessário para atender, por exemplo, a determinações legais, o interesse público e o direito de acesso à informação, são compatíveis com a LGPD, desde que adotadas as salvaguardas apropriadas.

Após tais apontamentos, destaca que a anonimização é uma das possíveis medidas de segurança que podem ser adotadas visando a proteção dos dados pessoais, citando ainda a pseudonimização, entre outras técnicas.

Não somente referente ao ENEM, mas de modo geral existem dados que precisam sofrer anonimização ou pseudonimização antes de serem divulgados a fim de evitar constrangimentos ao titular quando da divulgação das pesquisas.

Devem ser publicados apenas os dados que atendam às necessidades de cada ente, a exemplo dos que permitam a utilização em pesquisas acadêmicas, sem esquecer dos princípios relativos à proteção de dados pessoais e as normas de tratamento das legislações vigentes.

A própria divulgação consiste em tipo de tratamento previsto no art. 5º, X, da LGPD: "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".

Assim, já que a divulgação configura tratamento, faz-se mister que ela seja feita com respeito aos princípios previstos pela LGPD, de sorte a garantir que a

finalidade do tratamento seja atendida. Dessa forma, o fato de as informações públicas estarem disponíveis para uso sem consentimento deve motivar a reflexão sobre a publicação, a fim de que sejam divulgados apenas aqueles que sejam necessários e compatíveis com a realização de estatísticas e pesquisas científicas e com a execução da política pública de avaliação do sistema brasileiro de ensino que gerou o tratamento.

Ainda no material sobre a divulgação de microdados relativos ao ENEM, destaca-se:

> Miriam Wimmer, Diretora da ANPD, no artigo “O regime jurídico do tratamento de dados pessoais pelo Poder Público”, sugere a realização de relatórios de impacto à proteção de dados pessoais antes da abertura dos dados a serem publicados pelo Poder Público, e este é o posicionamento adotado pela ANPD no presente caso. Nessa senda, devem ser levados em consideração quais impactos a divulgação dos microdados pode causar aos direitos fundamentais ou no que a exposição pode afetar a vida dos indivíduos. No caso de dados identificáveis que podem, efetivamente, sujeitar o titular a discriminação, por exemplo, a publicação deve ser evitada, e em sendo necessária para política pública, o acesso deve ocorrer em ambiente seguro ou mediante a adoção de outras salvaguardas apropriadas. Assim, se o RIPD concluir que os dados são pessoais porque não estão anonimizados, entre a deliberação pela publicação e a publicação em si, deve haver reflexão sobre o que se precisa fazer. O documento, então, informará as precauções que a Autarquia federal tomará no intuito de mitigar os riscos às liberdades civis e aos direitos fundamentais[96].

A conclusão naquele material é de que os dados tratados se enquadram como dados pessoais por não estarem anonimizados, refletindo-se assim como serão tratados para evitar a ocorrência de incidentes. Do mesmo modo, conclui que a anonimização não é uma medida de segurança que deve ser adotada em todo e qualquer tratamento de dados pessoais, pois a LGPD não a elegeu como condição técnica para a divulgação pública ou para o compartilhamento de dados pessoais por entidades e órgãos públicos.

A principal determinação da LGPD é quanto à necessidade de avaliação de riscos e de adoção de medidas para mitigar a ocorrência de danos. Por

---

[96] ANPD. **Nota Técnica nº 46/2022/CGF/ANPD**. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000730_2022_53-nt-46.pdf.

esta razão, a eventual identificação dos titulares ou a admissão de algum grau de risco de sua identificação, quando necessário para atender, por exemplo, a determinações legais, o interesse público e o direito de acesso à informação, são compatíveis com a LGPD, desde que adotadas as salvaguardas apropriadas.

O grupo de trabalho para a proteção das pessoas no que diz respeito ao tratamento de dados pessoais instituído pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho adotou um parecer para analisar a eficácia e os limites das técnicas de anonimização existentes no contexto jurídico comunitário de proteção de dados e apresentar recomendações para lidar com essas técnicas, tendo em conta o risco residual de identificação inerente a cada uma delas.

Tal parecer foi adotado e 10 de abril de 2024, e esclarece que o GT reconhece o valor potencial da anonimização de dados pessoais, em particular enquanto estratégia para colher os benefícios dos denominados “dados abertos” para as pessoas e a sociedade em geral, reduzindo, simultaneamente, os riscos para as pessoas em causa.

Alguns estudos de caso e publicações científicas demonstraram a dificuldade de criar um conjunto de dados verdadeiramente anônimo que mantenha simultaneamente as informações subjacentes suficientes exigidas para a tarefa em questão.

As principais técnicas de anonimização de dados pessoais constam no referido parecer, em especial a aleatorização e a generalização. Aborda também a adição de ruído, a permuta, a privacidade diferencial, a agregação, o k-anonimato, a l-diversidade e a t-proximidade. Explica os seus princípios, os seus pontos fortes e fracos, bem como os erros e deficiências comuns relacionados com a utilização de cada técnica.

O parecer analisa a solidez de cada técnica com base em três critérios: se ainda é possível identificar uma pessoa, se ainda é possível estabelecer a ligação entre registos relativos a uma pessoa singular, e se podem ser inferidas informações relativamente a um indivíduo.

Criar um conjunto de dados verdadeiramente anónimo a partir de um conjunto substancial de dados pessoais mantendo, simultaneamente, as informações subjacentes exigidas para a tarefa não é um desafio simples.

O parecer conclui que as técnicas de anonimização podem fornecer garantias de privacidade e podem ser utilizadas para gerar processos eficazes de anonimização, mas apenas se a sua aplicação for adequadamente construída – o que significa que os requisitos prévios (âmbito) e os objetivos do processo de anonimização devem ser claramente definidos a fim de obter a anonimização pretendida, ao mesmo tempo que produzem alguns dados úteis.

Outro possível problema relativo à utilização da anonimização e pseudonimização para minimizar os efeitos de um incidente de dados é referente aos custos destes processos. Em pequenas empresas os custos podem variar de alguns milhares a dezenas de milhares de reais, dependendo das necessidades. Já em grandes organizações, pode-se falar em centenas de milhares de reais, especialmente se envolverem alta conformidade regulatória, grandes volumes de dados ou desenvolvimento personalizado.

Os colaboradores devem ser treinados para trabalhar com dados anonimizados/pseudonimizados, especialmente em setores sensíveis, o que por si só já acarreta custos, mesmo que não sejam implementados outros métodos.

O processamento de grandes volumes de dados pode exigir infraestrutura computacional robusta, por meio de servidores locais ou serviços de nuvem, e ainda pode haver custos com ferramentas de análise de dados, algoritmos de anonimização e pseudonimização, e segurança cibernética.

Os custos para anonimização e pseudonimização de dados podem variar amplamente, dependendo de vários fatores, como o volume de dados, a complexidade dos métodos utilizados e os recursos tecnológicos e humanos envolvidos.

Com relação ao volume, quanto maior a quantidade/volume de dados tratados, maior será o esforço e o custo associados ao processamento e à implementação das técnicas. Da mesma forma, dados complexos, com diferentes tipos (por exemplo texto, imagens, metadados, etc), exigem ferramentas e métodos especializados, o que também acaba por aumentar os custos. Além destes, dados desorganizados ou inconsistentes podem aumentar os custos devido à necessidade de limpeza e padronização antes da anonimização ou pseudonimização.

Softwares avançados para anonimização, como aqueles usados por

grandes empresas multinacionais, podem custar dezenas de milhares de dólares. Esses custos podem ser proibitivos para pequenas e médias empresas, que muitas vezes precisam buscar soluções mais acessíveis ou adaptar processos internos para lidar com dados sensíveis.

Para realização da anonimização, os processos podem ter custos variados. Pode-se adotar métodos simples, que são menos caros, como por exemplo a remoção de identificadores diretos, contudo pode ser que tais métodos não atendam completamente o fim desejado. Já técnicas mais avançadas como a supressão, perturbação de dados, entre outras, precisam de algoritmos mais sofisticados e, portanto, tem custos maiores.

A pseudonimização, por sua vez, envolve a substituição de identificadores diretos por chaves ou códigos, de forma que o custo aumenta se for necessário gerenciar sistemas de chaveamento e manter a reversibilidade de forma segura.

A implantação de k-anonimização e outras técnicas matemáticas pode demandar especialistas em ciência de dados, com custos variando conforme o volume de dados e a complexidade do processo. Em estudos na área de saúde, a pseudonimização com controle rigoroso pode ser mais cara devido à necessidade de manter dados identificadores separadamente em ambientes seguros e auditáveis.

Existem diversas ferramentas no mercado para anonimização e pseudonimização, de forma que os custos podem variar de licenças baratas para pequenas empresas até soluções corporativas mais caras. De maneira geral, o custo total envolve não apenas a tecnologia, mas também tempo, expertise técnica e atualizações constantes para mitigar riscos relacionados ao avanço tecnológico. Organizações maiores têm mais facilidade em absorver esses custos, enquanto empresas menores podem enfrentar desafios significativos para implementar soluções de conformidade.

A melhor solução deve ser decidida caso a caso, eventualmente por meio de uma combinação de técnicas diferentes e tendo em conta as recomendações práticas desenvolvidas no presente parecer. No que se refere a criar ferramentas personalizadas, geralmente envolve custos significativos com equipes de desenvolvimento, testes e manutenção.

Nisto se insere a figura do operador, que é quem irá realizar o tratamento de tais dados. Seu dever é realizar tal tratamento e conformidade com os parâmetros estabelecidos pelo operador, mas mais do que isso, tem o dever de tratá-los de forma a diminuir o risco de reidentificação e demais incidentes de segurança. Caso contrário, poderá sofrer as sanções previstas em lei e ser responsabilizado por suas condutas.

Assim, pode-se valer então o operador de dados dos processos de anonimização e pseudonimização durante o tratamento dos dados como uma medida de segurança adotada para evitar a ocorrência de incidentes. Até mesmo a simples manutenção do dado em sistema, desde que pseudonimizado, pode ser considerada uma medida de segurança, uma vez que em caso de ocorrência de invasão ao sistema, o atacante não conseguirá dados necessários para identificar os seus titulares e, assim, não conseguirá utilizar tais dados para fins não especificados no tratamento anteriormente consentido.

A atuação do operador de dados no tratamento é ativa, devendo se valer de todos os recursos a seu alcance para realizar tal tratamento em conformidade com as legislações vigentes, e de modo a assegurar também um armazenamento e descarte seguros do dado.

7 CONCLUSÃO

A Lei Geral de Proteção de Dados (LGPD) representa um marco regulatório no Brasil, buscando equilibrar a proteção dos direitos de privacidade dos indivíduos e as necessidades de uso de dados pelas organizações. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD introduz mecanismos para garantir a segurança de dados pessoais, especialmente diante do aumento dos incidentes de segurança. Entre essas ferramentas, destacam-se as técnicas de anonimização e pseudonimização, que têm como objetivo reduzir riscos associados ao uso indevido ou ao vazamento de informações.

A anonimização consiste em transformar dados pessoais de forma irreversível, eliminando a possibilidade de identificação dos titulares. Uma vez anonimizados, os dados deixam de ser considerados pessoais e, portanto, saem do escopo da LGPD. Já a pseudonimização, embora não retire o caráter de dado pessoal, dificulta significativamente a identificação ao substituir os identificadores originais por pseudônimos. Essa técnica, mais flexível, é amplamente utilizada em cenários onde é necessário preservar a utilidade dos dados enquanto se aumenta a segurança.

O estudo focou no papel do operador de dados na execução dessas técnicas, destacando sua responsabilidade em adotar medidas eficazes que estejam alinhadas às instruções do controlador e às exigências da LGPD. É importante ressaltar que nem todas as empresas possuem as figuras separadas de controlador e operador; em muitos casos, uma única entidade desempenha ambos os papéis. Quando presente, o operador atua diretamente na implementação de anonimização e pseudonimização, devendo garantir a aplicação de práticas que minimizem os impactos de incidentes de segurança.

Um dos desafios apontados é o custo envolvido nesses processos, que inclui aquisição de ferramentas tecnológicas, capacitação de profissionais, implementação de métodos técnicos e monitoramento contínuo. Esses custos, embora significativos, devem ser vistos como um investimento estratégico, dado o potencial de reduzir os danos financeiros e reputacionais decorrentes de um incidente de segurança. Eles exigem um compromisso contínuo com a atualização de ferramentas e capacitação de profissionais. Assim, a implementação dessas medidas não deve ser encarada apenas como um cumprimento legal, mas como um

investimento em segurança.

Embora a anonimização e a pseudonimização desempenhem papéis importantes na redução de riscos de vazamentos de dados, é crucial reconhecer que elas não oferecem uma proteção absoluta. Essas técnicas, por mais fundamentais que sejam, estão longe de serem soluções completas para os problemas de segurança cibernética que enfrentamos.

É fundamental que as organizações compreendam que a eficácia da anonimização e pseudonimização está longe de ser automática e depende de um contexto mais amplo de governança de dados. Essas ferramentas precisam ser complementadas por outras medidas de segurança.

A análise crítica revela que, embora não ofereçam proteção absoluta, a anonimização e a pseudonimização são fundamentais para mitigar riscos, sendo pilares importantes de um sistema de proteção eficaz. Contudo, é essencial que as organizações compreendam que essas técnicas não substituem outras medidas de segurança e que sua eficácia depende de atualizações constantes diante das evoluções tecnológicas.

No nível individual, essas práticas asseguram maior proteção à privacidade dos titulares em um ambiente digital interconectado. No nível organizacional, contribuem para minimizar os danos causados por vazamentos, protegendo tanto pessoas naturais quanto jurídicas. Por fim, conclui-se que o operador de dados desempenha um papel central nesse cenário, sendo indispensável que atue com diligência e em conformidade com os parâmetros legais, promovendo um ambiente digital mais seguro e confiável.

REFERÊNCIAS

AGGARWAL, Charu C.; YU, Philip S. **A general Survey of Privacy-Preserving Data Mining Models and Algorithms**. Privacy-Preserving Data Mining. Advances in Database System. vol 34. Springer. 2008. Acesso em: 30 set 23

AEPD-EDPS, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS – ***European Data Protection Supervisor. Misunderstandings Related to Anonymization***. Disponível em: https://edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en. Acesso em: 24 ago 23

AEPD-EDPS, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS - European Data Protection Supervisor. ***Orientaciones y garantías en los procedimientos de anonimización de datos personales****.* [S.l.]. AEPD, 2016. Acesso em: 30 set 23

ANACOM. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24.10.1995**. Disponível em: https://www.anacom.pt/render.jsp?contentId=965550. Acesso em: 30 set 23

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.** Brasília: ANPD, 2021. Acesso em: 24 ago 23

ANPD. **ANPD abre consulta à sociedade sobre o Guia de Anonimização e Pseudonimização**. 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-consulta-a-sociedade-sobre-o-guia-de-anonimizacao-e-pseudonimizacao. Acesso em: 24 ago 23

ANPD. **Consulta à Sociedade – Estudo Preliminar – Anonimização e pseudonimização para proteção de dados.** 2024. Disponível em: https://www.gov.br/participamaisbrasil/consulta-a-sociedade-estudo-preliminar-anonimizacao-e-pseudonimizacao-para-protecao-de-dados. Acesso em: 24 ago 23

ANPD. **ESTUDO PRELIMINAR. Anonimização e Pseudonimização para a proteção de dados pessoais**. 2023. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/37060. Acesso em: 24 ago 23

ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em: 24 ago 23

ANPD. **Guia Orientativo. Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas.** 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Acesso em: 24 ago 23

ANPD. **Guia orientativo – _Tratamento de dados pessoais pelo Poder Público.** [S.l.]: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 24 ago 23

ANPD. **Nota Técnica nº 46/2022/CGF/ANPD**. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000730_2022_53-nt-46.pdf. Acesso em: 24 ago 23

ANPD. **Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf. Acesso em: 24 ago 23

ARAGÃO, Alexandre. **5 grandes vazamentos de dados no Brasil — e suas consequências.** 2022. Disponível em: https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022. Acesso em: 15 dez 23

BBC. **O escândalo que fez o Facebook perder US$ 35 bilhões em horas**. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43466255. Acesso em: 15 dez 23

BESSA, Leonardo Roscoe. **A Lei Geral de Proteção de Dados e o direito à autodeterminação informativa**. 2020. Disponível em: https://www.conjur.com.br/2020-out-26/leonardo-bessa-lgpd-direito-autodeterminacao-informativa/. Acesso em: 01 jul 23

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020. Acesso em: 01 jul 23

BRAEKEN, A. **Public key versus symmetric key cryptography in client-server authentication protocols**. Int. J. Inf. Sec., v. 21, n. 1, p. 103–114, 2022. Disponível em: https://doi.org/10.1007/ s10207-021-00543-w. Acesso em: 15 dez 23

BRASIL. **DECRETO Nº 11.348, DE 1º DE JANEIRO DE 2023**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11348.htm. Acesso em: 01 jul 23

BRASIL. **LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 01 jul 23

BRASIL**. LEI Nº 10.406, DE 10 DE JANEIRO DE 2002.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 01 jul 23

BRASIL. **LEI Nº 12.414, DE 9 DE JUNHO DE 2011**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 01 jul 23

BRASIL. **LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 01 jul 23

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 01 jul 23

BRASIL. **LEI Nº 13.853, DE 8 DE JULHO DE 2019.** Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 01 jul 23

BRASIL. **MEDIDA PROVISÓRIA Nº 869, DE 27 DE DEZEMBRO DE 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 01 jul 23

CAPPELLO, Thamires. "Dos agentes de tratamento de dados pessoais". *In:* DANTAS, Eduardo *el al* (Coord.). **Comentários à Lei Geral de Proteção de Dados Sob a Perspectiva do Direito Médico e da Saúde.** Indaiatuba: Foco, 2023. Acesso em:

CARVALHO, A. P.; CANEDO, E. D.; CARVALHO, F. P.; CARVALHO, P. H. P. **Anonymisation and compliance to protection data: Impacts and challenges into big data.** In: FILIPE, J.; SMIALEK, M.; BRODSKY, A.; HAMMOUDI, S. (Ed.). Proceedings of the 22nd International Conference on Enterprise Information Systems, ICEIS 2020, Prague, Czech Republic, May 5-7, 2020, Volume 1. SCITEPRESS, 2020. p. 31–41. Disponível em: https://doi.org/10.5220/0009411100310041. Acesso em:

CASTELLS, Manuel. **A sociedade em rede**. Trad. Roneide Venâncio Majer. Vol. I. 6. Ed. Ver. Atual. São Paulo: Paz e Terra, 1999. Acesso em: 30 set 23

CHAVES, Luis. "Responsável pelo tratamento, subcontratante e DPO". *In:* MALDONADO, Viviane e OPICE BLUM, Renato. (Coord.) **Comentários ao GDPR [livro eletrônico]: regulamento Geral de Proteção de Dados da União Europeia**. 2ª Ed. São Paulo: Thomson Reuters, 2020. Acesso em: 15 dez 23

COELHO, Pablo Martins Bernardi, et al. **Responsabilidade dos provedores pelo tratamento dos dados sensíveis – Uma visão de acordo com as Leis de Proteção de Dados brasileira e europeia**. 2024. Disponível em: https://revistas.unimilitar.edu.co/index.php/dere/article/view/7053/5841. Acesso em:

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**, v. 13, p. 59-67, 2017. Acesso em: 15 dez 23

DATA PROTECTION COMMISSION. ***Guidance on Anonymization and Pseudonymization*** [S.l.]: DPC, 2019. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-

06/190614%20Anonymisation%20and%20Pseudonymisation.pdf. Acesso em: 30 set 23

DOU. **RESOLUÇÃO CD/ANPD Nº 18, DE 16 DE JULHO DE 2024**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074. Acesso em: 24 ago 23

EDPB. **Dados pessoais seguros.** Disponível em: https://www.edpb.europa.eu/sme-data-protection-guide/secure-personal-data_pt. Acesso em: 30 set 23

EUROPARL. **CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA**. 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 30 set 23

FRANCO, Paulo Alves. **Lei Geral de Proteção de Dados Comentada**. Leme, SP: Imperium Editora, 2020. Acesso em: 30 set 23

GARFINKEL, Simson L. **De-Identification of Personal Information**. [S.l.]: National Institute of Standards and Technology, 2015. p. 9.

G1. **Site eBay é vítima de ciberataque e recomenda mudança de senha.** 2014. Disponível em: https://g1.globo.com/tecnologia/noticia/2014/05/site-ebay-e-vitima-de-ciberataque-e-recomenda-mudanca-de-senha.html. Acesso em: 24 ago 23

G1. **Suspeitos do roubo das fotos de Carolina Dieckmann são descobertos**. 2012. Disponível em: https://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html. Acesso em: 24 ago 23

GDPR.EU. **Data Processing Agreement (Template).** Disponível em: https://gdpr.eu/data-processing-agreement/. Acesso em: 24 ago 23

GOV. **Incidentes de segurança com dados pessoais**. 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/semana-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais. Acesso em: 24 ago 23

GREENBERG, C. S.; MASON, L. P.; SADJADI, S. O.; REYNOLDS, D. A. **Two decades of speaker recognition evaluation at the national institute of standards and technology**. Comput. Speech Lang., v. 60, 2020. Disponível em: https://doi.org/10.1016/j.csl.2019.101032. Acesso em: 24 ago 23

GUNAWAN, D.; MAMBO, M. **Data anonymization for hiding personal tendency in set- valued database publication**. Future Internet, v. 11, n. 6, p. 138, 2019. Disponível em: https: //doi.org/10.3390/fi11060138. Acesso em: 30 set 23

HINTZBERGEN, Kees; HINTZBERGEN, Jule; BAARS, Hans. **Fundamentos de Segurança da Informação: com Base na ISO 27001 e na ISO 27002**. 1. ed. São Paulo: Brasport, 2018.

KRASTINS, Alexandra, et al. **Controlador ou Operador: quem sou eu? Cartilha sobre agentes de tratamento de dados pessoais.** 2021. Disponível em: 30 set 23https://lapin.org.br/wp-content/uploads/2021/04/Cartilha-Controlador-ou-Operador-quem-sou-eu-LAPIN.pdf. Acesso em: 24 ago 23

LI N.; LI, T.; VENKATASUBRAMANIAN S. **T-Closeness: Privacy Beyond k-Anonymity and L-Diversity**. IEEE 23rd International Conference on Data Engineering, 2007.

MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD Lei Geral de Proteção de Dados Comentada**. 2019. Revista dos Tribunais. 2. ed.

MARTELLO, Alexandre. **Banco Central comunica vazamento de dados de 53 mil chaves PIX da Qesh Instituição de Pagamento**. 2024. Disponível em: https://g1.globo.com/economia/noticia/2024/09/30/banco-central-comunica-vazamento-de-dados-de-53-mil-chaves-pix-da-qesh-instituicao-de-pagamento.ghtml. Acesso em: 12 nov 23

MÁXIMO, Wellton. **Banco Central comunica vazamento de dados de 39 mil chaves Pix.** 2024. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2024-07/banco-central-comunica-vazamento-de-dados-de-39-mil-chaves-pix. Acesso em: 12 nov 23

MENEZES CORDEIRO, A. Barreto. **Direito da proteção de dados: à luz do RGPD e da Lei 58/2019.** Coimbra: Almedina, 2020.

PASI, Renata Capriolli Zocatelli Queiroz; TEIXEIRA, Tarcisio. **Privacidade na internet: a formação de banco de dados e a transformação das pessoas em mercadorias.** Revista dos Tribunais nº 990, abril 2018.

QUEIROZ, Renata Capriolli Zocatelli. **A proteção de dados pessoais**: a LGPD e a disciplina jurídica do encarregado de proteção de dados pessoais. 2021. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2021. Disponível em: https://doi.org/10.11606/T.2.2021.tde-23082022-085834. Acesso em: 28 ago 23

REALE, Miguel. **Lições Preliminares de Direito**. 27 ed. Ver. Atual. Ajustada ao novo código civil. São Paulo: Saraiva, 2004.

REALE, Miguel. **Teoria Tridimensional do Direito**. 5 ed. rev. e aum. São Paulo: Saraiva,1994.

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

SAMARATI, P.; SWEENEY. L. **Protecting privacy when disclosing information: k-anonymity and tis enforcement through generalization and suppression**. Technical Report, 1998.

SCHWAB, Klaus. **A quarta revolução industrial**. Tradução Daniel Moreira Miranda. São Paulo: Edipro, 2016. Acesso em: 28 jan 23

SILVA, Lucas Henrique de Moura e. **Escolha da Criptografia Ideal e Anonimação de Dados Sensíveis Citados a Lei Geral de Proteção de Dados.** 2020. Disponível em: http://45.4.96.19/bitstream/aee/17213/1/TCC2%20WiLucasHenrique_Final.pdf. Acesso em: 27 out 23

SILVA, Salvador Márcio Rodriguesda; GOMES, Ana Carolina Nogueira; NAZARÉ, Tiago Bittencourt. **Lei Geral de Proteção de Dados: Métodos de Anonimização e Pseudonimização**. 2023. Disponível em: https://periodicos.unis.edu.br/mythos/article/view/804. Acesso em: 26 dez 23

SILVEIRA, Julia. **Documentos vazados mostram como o algoritmo do Google funciona; entenda**. 2024. Disponível em: https://www.techtudo.com.br/noticias/2024/06/documentos-vazados-mostram-como-o-algoritmo-do-google-funciona-entenda-edsoftwares.ghtml. Acesso em: 24 ago 23

SOUSA, Thiago do Rego; COUTINHO, Murilo; COUTINHO, Lilian; ALBUQUERQUE, Robson. **LGPD: Levantamento de Técnicas Criptográficas e de Anonimização para Proteção de Bases de Dados.** Sociedade Brasileira de Computação (SBC). 2020. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/19227/19056. Acesso em: 12 set 23

SPADONI, Pedro. **Vazamentos de dados atingem patamares assustadores em 2024, alerta relatório**. 2024. Disponível em: https://olhardigital.com.br/2024/07/18/seguranca/vazamentos-de-dados-atingem-patamares-assustadores-em-2024-alerta-relatorio/. Acesso em: 24 ago 23

STRIPE. **Data Processing Agreement – FAQS**. Disponível em: https://stripe.com/br/legal/dpa/faqs. Acesso em: 07 jul 23

TEIXEIRA, Tarcisio. **Curso de Direito e Processo Eletrônico: doutrina, jurisprudência e prática**. 4. ed. São Paulo: Saraiva, 2018

TEIXEIRA, Tarcisio, et al. **Lei Geral de Proteção de Dados Pessoais: comentada artigo por artigo**. 4. Ed. São Paulo: SaraivaJur, 2022.

TILT. **9,9 bi de senhas divulgadas: vazamento pode ser um dos maiores da história**. 2024. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2024/07/12/novo-vazamento-de-senhas-pode-ser-um-dos-maiores-da-historia.htm. Acesso em: 24 ago 23

União Europeia. **DIRETIVA 45/96/CE.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046. Acesso em: 15 nov 23

XAVIER, Fábio Correa. **Mãe de Todas as Violações: Entendendo o Maior Vazamento de Dados da História.** 2024. Disponível em: https://securityleaders.com.br/mae-de-todas-as-violacoes-entendendo-o-maior-vazamento-de-dados-da-historia/. Acesso em: 13 out 23