UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

SAMUEL LEAL VALENTIN

ESTUDO DE CASO: EXEMPLO DE APLICAÇÃO DA ANONIMIZAÇÃO EM UMA EMPRESA PÚBLICA BASEADO NA LGPD

CURITIBA

2023

SAMUEL LEAL VALENTIN

ESTUDO DE CASO: EXEMPLO DE APLICAÇÃO DA ANONIMIZAÇÃO EM UMA EMPRESA PÚBLICA BASEADO NA LGPD

Case Study: Example of Anonymization Implementation in a Public Company based on LGPD

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Bacharel em Sistemas de Informação do Curso de Bacharelado em Sistemas de Informação da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Leandro Batista de Almeida

CURITIBA

2023

SAMUEL LEAL VALENTIN

ESTUDO DE CASO: EXEMPLO DE APLICAÇÃO DA ANONIMIZAÇÃO EM UMA EMPRESA PÚBLICA BASEADO NA LGPD

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Bacharel em Sistemas de Informação do Curso de Bacharelado em Sistemas de Informação da Universidade Tecnológica Federal do Paraná.

Data de aprovação: 30/junho/2023

Leandro Batista de Almeida
Doutorado
Universidade Federal do Paraná

Fabiano Scriptore de Carvalho
Doutorado
Universidade Federal do Paraná

Christian Carlos Souza Mendes
Doutorado
Universidade Federal do Paraná

CURITIBA

2023

Dedico este trabalho à minha família e à minha noiva, que acompanharam toda minha caminhada na UTFPR e ajudaram nos momentos mais difíceis. Dedico também a Deus que permitiu que eu conquistasse a posição em que eu cheguei.

AGRADECIMENTOS

Gostaria de expressa minha gratidão a todos que estiveram presentes durante a produção deste trabalho. Em espacial gostaria de agradecer meu orientador prof. Leandro Batista de Almeida e o prof. José Antonio Buiar que auxiliaram na produção deste trabalho com suas orientações e indicações. Também expresso meu agredecimento aos professores participantes da banca que avaliaram meu trabalho.

Por fim, gostaria de agradecer a Universidade Tecnológica Federal do Paraná (UTFPR) de Curitiba por proporcionar minha formação acadêmica e permitir a realização deste estudo.

RESUMO

Segurança de dados e privacidade é um tema extremamente relevante para a atual sociedade, já que diariamente as pessoas têm seus dados coletados e processados por diversas organizações nacionais e internacionais. Para que exista controle com relação ao uso de dados pessoais, a Lei Geral de Proteção de Dados vem com o objetivo de trazer regras que garantam a segurança e a privacidade das pessoas. Como uma ferramenta que pode ser utilizada para o auxilio de segurança e conformidade com a lei, aparece a anonimização de dados. Este Trabalho tem como objetivo analisar o caso real e prático da empresa CELEPAR do estado do Paraná, procurando entender como funciona o processo de utilização da anonimização dentro da empresa, além de entender os seus desafios no meio interpessoal e limitações tecnológicas. Dessa maneira, foram encontrados dados interessantes desta aplicação estudada, observando o uso de licitação na contratação de um software, uso de anonimização na produção, manutenção e teste em sistemas, utilização de outros meios de segurança e privacidade além de desafios técnicos e interpessoais na adoção e utilização da ferramenta encontrada.

Palavras-chave: lgpd; anonimização; ciência de dados; segurança de dados; .

ABSTRACT

Data security and privacy are highly relevant topics in today's society, as individuals' data is collected and processed by numerous national and international organizations on a daily basis. The General Data Protection Law has been established to ensure control over the use of personal data and to establish rules that guarantee the security and privacy of individuals. Anonymization of data emerges as a tool that can assist in security and compliance with the law. This study aims to analyze a real and practical case of the CELEPAR company in the state of Paraná, seeking to understand the process of data anonymization within the organization. It also aims to comprehend the interpersonal challenges and technological limitations associated with its implementation. In this context, interesting findings were obtained from this case study, including the use of bidding for software procurement, the application of anonymization in system production, maintenance, and testing, the utilization of other security and privacy measures, as well as technical and interpersonal challenges encountered in the adoption and utilization of the identified tool.
Keywords: lgpd; anomization; data science; data security; .

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

Siglas

ACM	*Association for Computing Machinery*
ANPD	Autoridade Nacional de Proteção de Dados
DPA	*Data Processing Agreement*, do inglês Autoridade de Proteção de dados
DPO	*Data Protection Officer*, do inglês Encarregado de Proteção de Dados, de acordo com o encarregado da CELEPAR
EDPB	*European Data Protection Board*, do inglês Conselho Europeu para a Proteção de Dados
GDPR	*General Data Protection Regulation*, do inglês Regulamento Geral sobre a Proteção de Dado
IEEE	*Institute of Electrical and Electronics Engineers*
LGPD	Lei Geral de Proteção de Dados
SGSI	Sistema de Gestão de Segurança da Informação

SUMÁRIO

1 INTRODUÇÃO

A segurança e privacidade no mundo digital constituem um desafio complexo. Diariamente, uma quantidade incontável de informações são transmitidas em todo o mundo, incluindo dados que podem não ser relevantes para a maioria das pessoas. No entanto, em meio a essa enorme quantidade de dados, há uma quantidade significativa de informações sensíveis, como dados de saúde, finanças, lazer e outras áreas que envolvem diversas pessoas. À medida que esses dados são transmitidos pela internet e chegam às organizações, surge a questão crucial: como lidar com eles de maneira adequada e segura?

Com a coleta de dados de pessoas sendo feita todos os dias por diversas empresas das mais variadas áreas, viu-se a necessidade de se fazer algo para organizar e regulamentar o uso destes dados, pois não era possível dar uma liberdade que pudesse ferir o direito das pessoas. Dessa maneira, como é descrito pela autora (PINHEIRO, 2021), a União Europeia toma a liderança do debate deste problema, com a ajuda principalmente do partido *The Greens*, dando assim o surgimento da GDPR, em abril de 2016.

Com a GDPR surgindo, seu objetivo foi estabelecido como contribuir com a liberdade, segurança e justiça dentro da União Europeia, garantindo a transparência do tratamento de dados realizados dentro do bloco econômico para que exista a proteção das pessoas físicas, trazendo então efeitos políticos, econômicos e sociais. Mas isso, de acordo com (PINHEIRO, 2021), contribuiu para uma reação em cadeia, pois para que outras nações pelo mundo pudessem estabelecer comércios com a União Europeia, elas também deveriam ter Legislações equivalentes a GDPR.

Com a necessidade de existir uma Legislação do mesmo nível da GDPR, o Brasil então levantou a discussão sobre a LGPD. Antes dela, já existiram discussões como a do Marco Civil da Internet que surgiu em 2009 e foi transformado em lei em 2014, mas esta não apresentava tanto foco nos usos de dados pessoais. Depois do Marco Civil, ainda tiveram outras discussões não foram levadas com a seriedade necessária e nem tiveram grande objetividade, porém com o projeto de lei que veio a ser a LGPD foi diferente. Agora a discussão se tornou mais séria, sendo mais objetiva e clara no que seria proposto, dessa maneira a LGPD criou forma e se tornou algo real. (LORENZON, 2020)

Dentre várias recomendações e exigências que a LGPD e a GDPR trazem para as organizações, algumas dessa tem relação com a maneira em que os dados são armazenados, trazendo a obrigação de depois do uso dele ou excluir o dado ou utilizar um tipo de técnicas para que ele seja armazenado com segurança e não tenha como expor algum indivíduo, este tipo é a anonimização.(DONDA, 2020)

No contexto de organizações que lidam com dados sensíveis e são altamente impactadas com leis como a LGPD, existe a empresa pública CELEPAR. A Companhia de Tecnologia da Informação e Comunicação do Paraná (CELEPAR) é a primeira empresa pública de tecnologia da informação do Brasil, com a sua fundação no ano de 1964. O foco da empresa está na

sua missão de promover inovação e soluções tecnológica, melhorando a vida dos cidadãos e sendo referência no setor público. (CELEPAR, 2023b)

A empresa realiza serviços realizados para o governo do Paraná, além da procura por expandir seus serviços para outros estados também, com trabalhos relacionados com áreas como: Soluções para Governança e Gestão, Soluções de Suporte à Operação, Emissão certificação digital, serviços de *data center* e outros serviços. Dessa maneira, dentro do escopo nacional, é possível ver uma importância deles no setor de inovação nas empresas públicas.(CELEPAR, 2023a)

Assim, com tantos projetos e trabalhos ligados a setores públicos, é evidente a importância e influência da empresa com os dados pessoais dos cidadãos paranaenses, ocasionando também na necessidade de adoção de boas estratégias e ferramentas que auxiliem na segurança de dados. Considerando assim o escopo deste trabalho, utilizar ferramentas de anonimização de dados pode ser uma boa chave para o sucesso em proteger os dados pessoais em certas ocasiões.

1.1 Justificativas

Como a LGPD é uma legislação recente, muitos podem considerá-la um tema nebuloso, uma vez que ainda não teve tempo suficiente para se tornar comum no cotidiano. Entretanto, segundo a autora (PINHEIRO, 2021), seu cumprimento não é apenas uma opção para as empresas, mas uma responsabilidade e uma necessidade, haja vista que o não cumprimento das exigências da LGPD pode acarretar consequências graves, incluindo multas consideráveis para empresas de pequeno e médio porte. Além disso, a falta de cumprimento das exigências da LGPD pode ser vista como uma falha na segurança e uma vulnerabilidade dentro da organização, o que pode gerar uma imagem negativa para a empresa.

A ideia da LGPD de maneira geral é garantir o direito, segurança e privacidade aos usuários que disponibilizam seus dados aos clientes, então cumprir as exigências dela não pode ser vista como apenas uma lei passiva de punição, mas é possível enxergar uma maneira de garantir a qualidade do serviço prestado pela empresa. Assim, dentre várias situações em que as organizações precisam se enquadrar com a LGPD para dar esta qualidade na segurança e privacidade dos dados, uma delas está relacionada com as técnicas de anonimização dos dados.

Sabendo então que a LGPD está em vigor, não é algo extra na empresa e que ela é muito mais que punições para exigências não cumpridas. O que fazemos com a lei? Como posso saber se a organização está dentro das exigências da lei? Como posso utilizar esse tipo de técnicas anonimização para estar dentro da lei? Para auxiliar a resolver estas questões, este trabalho vem com o objetivo de entender a LGPD e suas exigências com relação ao tratamento de dados anonimizados e auxiliar profissionais da área a compreender em quais momentos é necessário e como aplicar as técnicas de anonimização.

1.2 Objetivos

1.2.1 Objetivo principal

Compreender a visão que a LGPD trás relacionada a anonimização de dados, trazendo algumas recomendações com boas práticas na aplicação da anonimização baseado em um estudo de caso.

1.2.2 Objetivo específico

- Realizar uma análise da visão da LGPD relacionada a anonimização de dados.
- Realizar uma entrevista com um funcionário que trabalha com processos de anonimização de dados dentro da CELEPAR.
- Analisar os resultados encontrados a partir da entrevista realizada e trazer as recomendações de boas práticas baseadas nesse estudo.

1.3 Estrutura do trabalho

Este trabalho está dividido em 5 partes. A primeira parte é esta seção de introdução, introduzindo o tema e esclarecendo o porquê deste tema e os objetivos que este trabalho propõe. A segunda parte é a do Referencial Teórico, que aborda um pouco mais aprofundado conceitos importantes que ajudaram a entender melhor o trabalho e o Estado da Arte. Já na terceira parte está a metodologia, em que foi abordado como foram feitas algumas partes do trabalho e como foi feito a parte de desenvolvimento das perguntas e da aplicação da entrevista, procurando contemplar todos os pontos que foram necessários para explicar de maneira total a escolha dos assuntos abordados. Por fim, a quarta e quinta parte são os resultados da entrevista e as considerações finais. Nesses dois últimos capítulos foram divididas reflexões com as questões que foram abordadas na entrevista. O objetivo foi compreender o que foi dito e como seria possível aplicar em outros casos semelhantes, observando os pontos negativos e positivos do uso de anonimização e as suas questões de segurança.

2 REFERENCIAL TEÓRICO

Neste capítulo será abordado mais profundamente os temas da LGPD e a GDPR, além de abordar leis e problemas que originaram estas legislações. O objetivo é ajudar em um melhor entendimento do trabalho, explicando o funcionamento e conceitos relacionados a estes temas. Ainda também, será abordado conceitos ligados a Privacidade e Segurança que também serão importantes para entendermos a importância de tudo isso. Por fim, será abordado o Estado da Arte.

2.1 Leis anteriores

2.1.1 Classificação de Viktor Mayer-Scönberger

Na busca de entender como foi o processo evolutivo das leis que originaram as GDPR e LGPD que conhecemos hoje, podemos nos basear na classificação das gerações de lei feito pelo alemão (MAYER-SCÖNBERGER, 1997). A classificação deste autor feita no ano de 1997 está dividida em 4 gerações, indo de leis com um foco muito fechado na tecnologia e indo até as leis que se assemelham mais às leis como a GDPR, apesar dos anos de diferença.

A primeira geração de leis foi existiu até meados da década de 70 e tinha o objetivo de regular a coleta e gestão dos dados pessoais, que na época eram concentrados em Centros elaboradores de dados. O foco principal destas leis era na autorização para criação desses bancos de dados e o seu controle feito por órgãos públicos, enfatizando então o controle do uso destes dados pessoais pelo estado. Problemas destas lei como o foco no Banco de dados e não na privacidade destes dados de fato além de pouca familiaridade com as tecnologias, fez com que não demorasse muito para que elas ficassem obsoletas com a multiplicação dos centros de tratamento de dados.(GALVAO, 2021)

Com as leis da primeira geração ficando ultrapassadas no final dos anos 70, a segunda geração de leis começou a surgir, podendo apontar a lei Francesa de Proteção de Dados Pessoais, chamada de *Informatique et Libertées*, como um grande exemplo desta nova geração. Diferente das leis passadas que o foco era a parte computacional do banco de dados, o foco agora é na consideração da privacidade e na proteção de dados. Essa mudança veio diretamente da insatisfação dos usuários que sofriam com o uso dos seus dados por terceiros sem a existência de ferramentas que pudessem dar a chance do próprio cidadão exercer seu direito de proteção dos seus dados pessoais.(DONEDA, 2011)

Já a terceira geração destas leis surgiu durante a década de 80, ainda com o foco do cidadão ter direito com os seus dados, mas agora esta geração abrange mais do que a liberdade de fornecer ou não os dados pessoais, mas agora também tem o foco em garantir a liberdade de maneira mais geral no processo. A proteção de dados é mais complexa agora, envolvendo mais

parte do processo além da liberação do uso inicial, procuravam agora incluir as fases sucessivas do processo de tratamento e utilização das informações por parte de terceiros.(BURILLE, 2022)

Por fim, a quarta geração vai até as leis no final da década de 90, quando o (MAYER-SCÖNBERGER, 1997) escreveu esta classificação. A última geração surgiu com o foco em diminuir a desvantagem individual que existia na época, dando mais força para as pessoas em relação às entidades de coleta de dados. Além disso, estas leis traziam normas que eram específicas para determinados setores de processamento de dados como por exemplo o setor de saúde. Um dos exemplos que podemos dar desta quarta geração de lei é a Diretiva 2000/58/CE, conhecida também como Diretiva sobre privacidade e as comunicações eletrônicas.(DONEDA, 2011)

2.2 Regulamento Geral sobre a Proteção de Dado - GDPR

A Regulamentação Geral da Proteção de Dados europeia pode ser vista como uma grande pioneira neste assunto de privacidade digital. Além disso, ela acaba sendo uma grande influência para diversas outras regulamentações, incluindo a nossa própria LGPD, principalmente por ser muito completa e bem estruturada. Uma das principais bases deste regulamento é a importância do consentimento do usuário com tratamento dos seus dados pessoais feito por empresas públicas e privadas, trazendo a necessidade de que estes processos de tratamento de dados sejam bem claros mesmo antes da coleta ser feita.

2.2.1 Definições

É importante entender como a GDPR define o que é dado pessoal. Assim, na visão dela toda informação que consegue se relacionar com uma pessoa física identificado ou identificável, sendo dados físicos ou digitais, é um dado pessoal. Dessa maneira, o dado será considerado pessoal se for possível identificar uma pessoa através destes dados. Assim, a definição de dados pessoais pode se manter mais geral e atemporal, evitando que ela se torne obsoleta com facilidade.(VOIGT, 2017)

Olhando agora como essa legislação define o processamento, podemos entender que a definição se resume em qualquer operação ou conjunto de operações realizadas com o uso de dados pessoais. Esta definição também independe do processamento ser em forma de coleta, armazenamento, registro, estruturação, alteração, consulta, divulgação, de maneira automatizada e de outros tipos de processamento que podemos ver no artigo 4 da (GDPR, 2016).

Além da definição de dados pessoais e processamento, devemos ressaltar que a GDPR não dá a propriedade sobre os dados pessoais para o usuário, mas dá a ele o direito e o controle do que será feito com estes dados, dessa maneira o usuário tem o direito de saber o que vai ser feito, mas ele não é dono propriamente dito destes dados. Porém, mesmo que a unidade

onde será feito o processamento desses dados já tenha o direito de usar os dados pessoais, como o cidadão deve saber o que será feito com eles, caso exista alguma mudança do que fora combinado previamente entre organização e cliente, deverá ser informado ao cidadão de maneira adequada. (NEVES, 2021)

2.2.2 Aplicabilidade

Outro ponto interessante da GDPR é a extraterritorialidade da aplicabilidade das diretrizes desta Legislação, que envolve qualquer indivíduo que faz parte da União Europeia ou de dados que estão no território da UE. Dessa maneira então, qualquer dado que for processado que tenha relação com a União Europeia mesmo que a sua origem venha de outro lugar, o processo de tratamento de dados precisa estar de acordo com as diretrizes estabelecidas pela GDPR. Esse ponto é muito importante por nos mostrar a razão da necessidade de que qualquer país que pretende estabelecer relações comerciais com a Europa, precisa de uma legislação que se assemelhe a legislação europeia de proteção de dados. (GALVAO, 2021)

2.2.3 Encarregados de proteção de dados - DPO

Antes da chegada da GDPR a necessidade de criação do cargo *Data Protection Officer*, do inglês Encarregado de Proteção de Dados, de acordo com o encarregado da CELEPAR (DPO) não era tão difundido entre os estados participantes da União Europeia, porém a nomeação deste cargo existe há décadas na Alemanha, onde este tipo de profissional se mostrou muito eficaz, agora então na GDPR o profissional designado a ser o DPO tem um grande papel na conformidade da organização com esta regulamentação. Entre as competências que um profissional para este cargo deve ter estão: conhecimento especializado sobre as leis e proteção de dados e também a capacidade de cumprir com as responsabilidades legais.(VOIGT, 2017)

As responsabilidades atribuídas ao DPO são: informar e aconselhar o processador de dados e seus funcionários quanto a obrigações de proteção, monitorar as conformidades com a regulamentação do processador de dados, aconselhar sobre o impacto gerado na proteção de dados e acompanhar seu desempenho, cooperar com a autoridade supervisora e por fim ser o ponto de contato entre a organização e a autoridade supervisora.(NEVES, 2021)

2.2.4 Autoridade de proteção de dados - DPA

Além do DPO, a GDPR traz a ideia da criação de uma autoridade existente para cada estado membro da União Europeia. Dessa maneira, cada estado estabelece um conselho que será seu *Data Processing Agreement*, do inglês Autoridade de Proteção de dados (DPA) e também irá indicar quais são os direitos e poderes estabelecidos a eles de acordo com a leis

daquele estado. Também será garantido o poder para as DPA de aplicar punições aos que não estiverem de acordo com as diretrizes da regulamentação, o que também irá poder variar de acordo com as leis de cada estado. (LORENZON, 2020)

2.2.5 Conselho Europeu para a Proteção de dados - EDPB

Por fim, com o objetivo de implementar de maneira consistente a GDPR por toda a UE, foi criado o *European Data Protection Board*, do inglês Conselho Europeu para a Proteção de Dados (EDPB) composto por representantes das DPAs, com o objetivo de emitir diretrizes e tornar a aplicação da GDPR uniforme entre todos os países membros, sem que exista diferenças nas aplicações de acordo com diferente jurisdições. (LORENZON, 2020)

2.3 Lei Geral de Proteção de Dados - LGPD

Muito recentemente no Brasil, mais precisamente em 2018, foi aprovada então a lei Nº 13.709, de 2018, conhecido como a LGPD que está vigente em suas disposições gerais desde setembro de 2020, mas a aplicações de punições para os que não estiverem de acordo com as exigências da lei começaram a ser feitas a partir de agosto de 2021. Porém, desde antes das empresas serem passíveis de punições pela falta de conformidade com a Lei, qualquer usuário proprietário dos dados utilizados por empresas já possuía total direito de questionar empresas privadas e órgãos públicos sobre como eram feitos os processos de tratamento de dados pessoais.

A LGPD pode ser considerada menor que a GDPR, já que ela possui 10 capítulos e 65 artigos, enquanto a GDPR possui 11 capítulos e 99 artigos. Tornando então a nossa versão nacional mais enxuta, além de às vezes deixar uma margem de interpretação na sua aplicabilidade, por exemplo a GDPR deixar claro prazos para determinadas situações enquanto a LGPD traz "prazos razoável". (PINHEIRO, 2021)

2.3.1 Constituição e Objetivo

Baseando-se na própria descrição da lei no Art. 1º Lei nº 13.853, de 8 de julho de 2019, "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."(BRASIL, 2019).

Além da lei nº 13.853, de 8 de julho de 2019(BRASIL, 2019), ainda trazer em seu Art. 2º quais são os seus pilares:

1. O respeito à privacidade.

2. A autodeterminação informativa.
3. A liberdade de expressão, de informação, de comunicação e de opinião.
4. A inviolabilidade da intimidade, da honra e da imagem.
5. O desenvolvimento econômico e tecnológico e a inovação.
6. A livre iniciativa, a livre concorrência e a defesa do consumidor.
7. Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Fica explícito como o objetivo da lei é a de regulamentar o tratamento de dados no Brasil, com o objetivo de proteger a privacidade e os direitos dos indivíduos que têm seus dados processados ou coletados em território nacional. A LGPD busca dar maior controle e liberdade aos titulares dos dados com suas informações pessoais, além de visar trazer uma maior transparência no tratamento de dados, estabelecendo a necessidade das empresas serem mais claras e acessíveis com seus objetivos e métodos perante o uso de dados que eles coletaram.(GALVAO, 2021)

2.3.2 Definições

Assim como a GDPR, a nossa LGPD também traz algumas definições importante, por exemplo a de Tratamento de dados, sendo ela bem parecida com a sua versão da GDPR de ser qualquer operação realizada com o uso de dados pessoais podendo ser: transmissão, processamento, coleta, produção, acesso, avaliação, edição modificação e outros tipos. Dessa maneira então, é estabelecido na LGPD que qualquer pessoa que trate de dados nessa definição ampla, podendo ser de direito público ou privado, natural ou jurídica, deverá ter bases legais para fundamentar este processo de tratamento de dados pessoais que ela pretende realizar.(TEFFE; VIOLA, 2020)

Além do tratamento de dados, outra definição semelhante é a de dados pessoais, que é qualquer informação relacionada a uma pessoa identificável ou identificada como nome, endereço, localização e outros que pode relacionar a uma pessoa física direta ou indiretamente. Esse conceito amplo do que é dado pessoal vem diretamente da regulamentação europeia, assim, mesmo que o dado pareça irrelevante no primeiro momento, ele pode nos trazer informações pessoais depois do uso de certos tratamentos para aquele dado.(TEFFE; VIOLA, 2020)

Mas a LGPD ainda traz outras definições como a de Dados Pessoais Sensíveis que são informações ligadas a características da personalidade e escolhas pessoais de um indivíduo, além de dados anônimos que são dados relativos a um indivíduo que não pode ser identificado considerando os meios possíveis durante o tratamento e o de anonimização que são técnicas

usadas durante o processamento de dados para tirar a possibilidade de associar o dado diretamente ou indiretamente a um indivíduo.(LIMA, 2020)

2.3.3 Deveres das organizações

Assim como na GDPR, a LGPD traz para as organizações também a necessidade de profissionais para ajudar a deixar os processos conforme é exigido nas diretrizes. Então o cargo de DPO é de extrema importância assim como na regulamentação europeia, liderando uma equipe a fim de organizar as ações de proteção e análise de dados. Mesmo que para uma empresa seja difícil a contratação de um profissional para a realização desta tarefa, é necessário que exista pelo menos uma pessoa que seja designada para esta função. Assim, este profissional fica responsável pelos agentes de tratamento que são definidos como controlador e operador de acordo com a própria LGPD.(DONDA, 2020)

2.3.4 Autoridades

Como a LGPD está em âmbito nacional e a GDPR funciona em um bloco de países, acaba acontecendo algumas diferenças como a não aparição da EDPB na LGPD. Porém, a lei brasileira cita a Autoridade Nacional de Proteção de Dados (ANPD), que seria o equivalente a DPA da GDPR. A ANPD possui diversos poderes em comum com a sua equivalente europeia, para que seja possível a realização da suas tarefas, por exemplo: poder de investigação exigindo informações para que seja averiguado possíveis infrações, poder de correção através de aplicações de punições, bloqueios e advertências para as organizações e por fim a autoridade deve promover consulta ao analisar as reclamações dos titulares dos dados. (NEVES, 2021)

Como é dito na própria lei nº 13.853, de 8 de julho de 2019(BRASIL, 2019), em seu Art. 5º a definição de Autoridade Nacional é: "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional."

No geral, a ANPD é bem semelhante com a DPA da Europa, com o objetivo de difundir e promover ao público nacional uma preocupação com a proteção de dados pessoais. Contribuindo isto com realização de estudos de práticas nas organizações com relação a proteção e direito à privacidade. (GALVAO, 2021)

2.3.5 Aplicabilidade da lei

A aplicabilidade da LGPD pode ser visto como ampla assim como a GDPR é, se aplicando para todas as organizações sendo elas públicas ou privadas e pessoas físicas ou jurídicas que fazem o tratamento de dados pessoais com qualquer tipo de operação se elas ocorrerem em umas dessas situações: se elas estiverem ocorrendo em território nacional, se

o objetivo final ou o tratamento dos dados estiverem em território nacional e por fim se os dados forem coletados em território nacional. Em casos de pessoas naturais que não possuam fins econômicos e tenham também fins exclusivamente particulares, a lei não se aplicará. Além disso, existem outros casos que também a lei não se aplica, como para fins jornalístico, artístico, acadêmico, defesa nacional e outros.(NEVES, 2021)

Dessa maneira, a LGPD pode ter um alcance internacional, já que ela não está presa exclusivamente em processos que ocorrem dentro do Brasil, mas está no alcance de qualquer processamento de dados pessoais que envolvem o território nacional. Porém, em casos como o tratamento de dados por parte de um pessoa física que utiliza eles para usos exclusivamente jornalísticos, artísticos, particulares e não econômicos e para fins de segurança pública, a lei não será aplicada.(PINHEIRO, 2021)

2.3.6 Ações corretivas da lei

Uma preocupação relevante para as organizações com a LGPD são as suas possíveis punições, advertências e multas. Podemos observar então na lei nº 13.853, de 8 de julho de 2019(BRASIL, 2019), em seu Art. 52º como exemplo as cinco primeiras possíveis medidas aplicáveis são de:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2 % (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

Ou seja, além de danos financeiros que podem ser altos, ainda existe a possibilidade de bloqueio dos dados da infração, que para aquela organização pode ser importantíssimo. Porém, é claro que cada situação vai possuir diferentes conclusões na questão de ações corretivas, cabe a responsabilidade de decidir a medida a ANPD, para que seja justo com as possíveis ações tomadas até a resolução do problema.(NEVES, 2021)

2.4 Anonimização

Como o foco deste trabalho está na aplicação da anonimização, é importante ressaltar a visão da LGPD com este tema. Mais adiante deste trabalho, será citado a visão da LGPD

com este tema baseado nos trabalhos(PINHEIRO, 2021) e (BIONI, 2020), considerando as suas definições e recomendações. Porém, é importante citar o que de fato a lei traz, assim, foi observado que a as palavras anonimização e anonimizado aparecem quatorze vezes e a palavra pseudonimização aparece duas vezes na lei nº 13.853, de 8 de julho de 2019(BRASIL, 2019), mostrando sua importância e ligação com a lei.

Nas duas primeiras citações a este tema na lei, aparecem as definições de dado anonimizado e anonimização no Art. 5º. Sendo a definição de dado anonimizado: 'dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;' e a definição de anonimização: '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;' (BRASIL, 2019).

Nesse mesmo Art. 5º, ainda aparecem outras definições importantes como a de dados pessoais, dados pessoais sensíveis, controlador, operador, encarregado entre outros. Estas definições são importantíssimas para entender o que a lei compreende em suas questões.

As próximas duas aparições destas palavras relacionadas com este tema estão nos Art. 7º e no Art. 11º, sendo relacionado respectivamente com o tratamento de dados pessoais e dados pessoais sensíveis. Nestes dois casos é citado a garantia do uso de anonimização destes dados sempre que possível, na realização de estudos por órgão de pesquisa. Ainda na questão de órgãos de pesquisa, a lei traz também no seu Art. 13º a garantia do uso de anonimização sempre que possível também em estudos na área de saúde pública realizadas por o órgãos de pesquisa.(BRASIL, 2019)

Depois dessas citações, este tema aparece novamente para definir uma questão importante no uso de anonimização por parte das organizações. Assim então, o Art. 12º fala: 'Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.'(BRASIL, 2019)

Este trecho citado da LGPD mostra o porquê da anonimização ser uma ferramenta importante para a conformidade com a lei. Considerando então que se o processo da anonimização não puder ser revertido de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios, este dados não serão tratados como dados pessoais sensíveis. Ou seja, mesmo que a organização ainda precise destes dados para alguma estratégia e permaneça com eles armazenados, se eles forem devidamente anonimizados, a empresa poderá estar em conformidade com a lei.

Indo para as questões após o término do tratamento de dados. este tema aparece mais duas vezes em seu Art. 16º, exigindo a garantia do uso de anonimização sempre que possível para os órgãos de pesquisa e trazendo e exigência de 'uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.' para as organizações. (BRASIL, 2019)

Por fim, as últimas citações deste tema na lei se dão para o direito do titular dos dados. Assim no Art. 18º é mostrado o direito do titular dos dados de requisitar a anonimização de seus dados, além de exigir que: 'O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento,'(BRASIL, 2019)

Na questão da palavra pseudonimização, a aparição dela está apenas no Art. 13º. Sendo a primeira citação relacionada com a questão de estudos na área de saúde pública feita por órgãos de pesquisa, sendo uma recomendação. A última citação é a definição do que seria a pseudonimização, sendo descrito como: 'é o tratamento por meio do qual um dado 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.'(BRASIL, 2019)

No geral, como foi descrito anteriormente, a LGPD traz a anonimização como uma recomendação em alguns casos e também como um solução, para que a lei não se aplique em determinados dados. Dessa maneira, dentro da visão da LGPD é possível ver a utilidade da anonimização para as empresas, sendo um auxílio para que exista uma conformidade completa com a lei.

2.5 Comparação entre LGPD e GDPR

A tabela abaixo nos traz uma comparação direta entre as duas principais legislações apresentadas neste trabalho. Existir essa comparação mais direta e prática em formato de uma tabela, ajuda a tornar mais visível as diferenças e semelhanças. As informações descritas nesta tabela são baseadas nas seções de LGPD e GDPR deste trabalho, mas podemos observar nos trabalho das autoras (LORENZON, 2020) e (NEVES, 2021), que fazem a comparação das duas legislações e falam sobre as diferenças entre as multas, definição de dado pessoal, aplicabilidade e responsabilidades.

Tabela 1 – Quadro comparativo entre as Legislações GDPR e LGPD

Aspectos	GDPR	LGPD
Data de entrada em vigor	25 de maio de 2018	18 de setembro de 2020
Local de origem	União Européia	Brasil
Áreas de aplicação	Qualquer indivíduo que faz parte da União Europeia ou de dados que estão no território da UE.	Para todas as organizações e pessoas físicas ou jurídicas que coletam e processam dados no Brasil
Definição de dados pessoais	Qualquer informação que possa identificar um indivíduo direta ou indiretamente	Qualquer informação relacionada a uma pessoa natural identificada ou identificável
Multas	As multas podem chegar a 20 milhões de euros ou 4 % do faturamento global anual da empresa.	As multas podem chegar a 2 % do faturamento bruto da empresa no último exercício fiscal, limitado a 50 milhões de reais por infração
Responsabilidades	A responsabilidade do processamento de dados é tanto dos controladores quanto dos processadores de dados.	A responsabilidade do processamento de dados é dos controladores deste dados.

Fonte: Autoria própria.

2.6 Normas ISO

Com este trabalho está relacionado com assuntos como anonimização e LGPD em organizações, o tema segurança da informação pode ser visto como o assunto central deste texto. Assim, é necessário também citar as normas ISO 27001 e 27002, que tratam diretamente deste tema de segurança. Dessa maneira, com o intuito de aprofundar a compreensão das questões relacionadas à segurança da informação, este estudo abordará as questões estabelecidas nas normas ISO 27001 e ISO 27002. A proposta desta seção é explorar as principais áreas e questões abordadas por cada norma.

2.6.1 ISO 27001

A proposta da norma ISO 27001 é a de auxiliar os vários tipos de organizações de qualquer área na proteção de suas informações, usando meios econômicos de forma sistemática, usando a adoção de um Sistema de Gestão de Segurança da Informação (SGSI). Além disso, a norma não pretende apenas ensinar as empresas a realizar ações para o auxílio da segurança das informações, mas a ISO também oferece a possibilidade da empresa conseguir uma certificação, que irá dar uma segurança e uma prova de que a empresa consegue fornecer uma

segurança de seus dados. Como as normas ISO são reconhecidos por todo o mundo, a obtenção de certificações e de usos de suas boas práticas são uma boa maneira de abrir novas portas para negócios no mundo inteiro.(SOUZA, 2008)

Dentro do funcionamento da norma ISO 27001, o foco fica na proteção da confiabilidade, integridade e disponibilidade das informações dentro da empresa. O processo para se chegar nessa proteção é por meio de uma avaliação de potenciais riscos que podem acontecer com as informações, para depois definir o que é necessário para evitar os problemas potenciais. No geral podemos observar uma filosofia de gestão de riscos, indo do ponto de encontrar as vulnerabilidades e problemas até o ponto de tratar cada caso sistematicamente.(MAGALHãES, 2021)

Para que uma organização seja considerada dentro das conformidades da norma ISO 27001, ela precisa cumprir com os seus requisitos obrigatórios. Estes requisitos são definidos em áreas, descritas nas cláusulas da norma, sendo dividido nos seguintes grupos: contexto da organização, liderança, planeamento, suporte, operação, avaliação de desempenho e melhorias. Além desses requisitos, para que seja possível a implantação da norma em uma organização, são implementados controles técnicos, organizacionais, legais, físicos e de recursos humanos.(MAGALHãES, 2021)

2.6.2 ISO 27002

De maneira complementar a norma ISO 27001, aparece a norma 27002 para auxiliar na segurança da informação de maneira mais direta. Enquanto a primeira norma foca na gestão dos riscos na proteção das informações das organizações, a ISO 27002 vem como uma norma focada em boas práticas que irão assegurar a segurança dos dados, aplicadas por meio de um SGSI. (MATTES; PETRI; ROSA, 2015)

Esta norma tem como finalidade trazer recomendações, para que as pessoas que são encarregadas de escolher e implementar a segurança da informação, tenham boas práticas e ações para a implementar as qualidades desta norma na organização(MAGALHãES, 2021)

Seguindo então essa proposta de recomendar ações que sejam boas práticas para assegurar a proteção da informação, a norma ISO 27002 traz como alguns dos seus requisitos pontos como: gerenciamento das operações e comunicações, classificação e controle de ativos da informação, segurança ambiental e física, controle de acesso, segurança relacionada às pessoas e política de segurança. Esses requisitos tentam abordar questões que envolvem a parte física e tecnológica, procurando organizar e prevenir problemas em diversos escopos.(JUNIOR; SANTOS; ALBUQUERQUE, 2014)

Dentro desta norma também existe a aplicação de diversos controles assim como foi descrito na norma anterior, existindo inclusive controles com mais de uma função. Porém, o texto da norma traz a ideia de que o conjunto de controles não é totalmente abrangente, pois cada organização e contexto exigem uma maneira diferente de se aplicar controles, podendo variar

muito em cada caso. Sendo assim, a norma traz uma visão ampla de adaptação. (MAGALHãES, 2021)

2.6.3 ISO 27701

No geral, as normas ISO da família 27000, foram atualizadas e adaptadas para estarem de acordo com as exigências da GDPR, para que seja estabelecido mais orientações essenciais, melhorando a segurança e a contenção dos riscos relacionados à utilização de dados pessoais. Com estas mudanças para a lei europeia, surgiram também mudanças nas normas ISO para a conformidade com a LGPD. Assim, em 2019 apareceu a norma ISO/IEC 27701:2019, buscando resolver as questões relacionadas com as leis atuais(ANDRADE; KIM, 2019)

Esta norma pode ser vista como uma extensão da 27001, tendo como seus requisitos e diretrizes finalidades relacionadas ao estabelecimento, implantação, manutenção e melhoria constante de um sistema de gestão de privacidade da informação. A finalidade desta ISO é a de auxiliar empresas a demonstrar sua preocupação e esforço para adquirir eficientemente as melhores práticas internacionais na questão de proteção de dados.(JESUS, 2022)

Além de complemento da 27001, a norma ISO 27701 também adiciona diretrizes para certos pontos que também são tratados na ISO 27002, podendo ser vista como pontos estendidos. Podemos observar nos exemplos das seções de políticas de segurança da informação, organização da segurança da informação, segurança em recursos humano, gestão de ativos, segurança das comunicações, segurança física e de criptografia e na gestão de incidentes de segurança, em que a norma ISO 27002 pode ser estendida e complementada com a ISO 27701.(DELAGUSTINHI, 2021)

Porém, além de complemento, a norma ISO 27701 também possui diretrizes próprias para o SGSI. Esta norma tem como um dos seus objetivos assegurar que a organização seja totalmente clara nas suas declarações de consentimento, políticas e procedimentos no tratamento de dados, para que não tenha nenhum tipo de ambiguidade para os titulares dos dados tratados, entregando uma maior segurança no consentimento entregue pelos titulares.(DELAGUSTINHI, 2021)

A norma 27701 também oferece um anexo com um mapeamento sobre a LGPD, podendo auxiliar as organizações com suas conformidades com a lei no Brasil.(DELAGUSTINHI, 2021) Observamos também a relação com a anonimização, podendo aparecer nas políticas de tratamento de dados, tornando assim esta norma importantíssima para este trabalho, relacionada com a LGPD e a anonimização.(FAL', 2021)

2.6.4 Diferenças e finalidades

No geral, as diferenças entre as três normas estão na abordagem para a mesma situação. Como foi dito na seção anterior as três são complementares, porém, podemos definir a principal diferença das normas como a ISO 27001 para a gestão de riscos utilizando a identificação de riscos e implantação de mitigação, enquanto na ISO 27002 temos boas práticas que serão aplicadas na gestão de segurança da informação feita com a norma anterior, por fim a ISO 27701 é muito relacionada com a LGPD e possui um foco em garantir a privacidade da informação(MAGALHãES, 2021)

Para que uma empresa tenha uma segurança maior de suas informações, tanto para conquistar uma imagem pública positiva em negociações quanto na segurança de fato de seus dados, estas três normas ISO são uma ótima ferramenta. Existem outras maneiras também de garantir uma segurança dentro de uma organização, entretanto, a influência e importância no mundo corporativo que as normas ISO conquistaram, colocam elas em uma posição de vantagem para serem adotadas.(MATTES; PETRI; ROSA, 2015)

2.7 Anonimização

Um dos problemas existentes em organizações que são controladoras de dados é o equilíbrio entre a segurança do armazenamento e a utilidade destes dados. Apenas armazenar todos os dados coletados pode trazer algumas utilidades, como por exemplo uma análise estatística para estratégias da organização. Porém, possuir estes dados dentro de um banco de dados controlado por uma organização também traz uma série de responsabilidades, pois um possível vazamento ou um uso indevido destes dados poderia acarretar em uma perda de reputação grande para a empresa.(BOMFIM, 2017)

Uma ótima solução para encontrar esse equilíbrio seria o uso de anonimização de dados. Transformando os dados em anonimizados, podemos dissociá-los dos seus respectivos titulares, mas ainda deixá-los úteis para o uso dentro dos sistemas das organizações e ainda permanecer em conformidade com a lei. Para realizar esses procedimentos, poderão ser utilizados diversos procedimentos e técnicas que possam auxiliar nessa dissociação, normalmente utilizando de eliminação de elementos desses dados que possam ser identificadores dos seus titulares.(JúNIOR; MARTINS, 2021a)

Podemos observar o uso de anonimização em algumas situações, em que cada uma pode utilizar uma abordagem e técnica diferente. Um exemplo de situação é o do uso para proteger os dados que vão ser usados em produção de desenvolvimento de *software* ou análise estatística dos dados, nesse caso os dados são anonimizados para serem utilizados por programadores ou estatísticos que precisam do acesso. Outro exemplo seria o uso para a proteção de dados dentro de um banco de dados, diminuindo os risco de alguém conseguir acessar estes dados e tirar informações sensíveis destes dados. (SOUSA *et al.*, 2020a)

2.7.1 Definição da LGPD

É importante apontar duas definições na visão da LGPD, a de anonimização, de dado anonimizado. A LGPD define anonimização como o processo que utiliza meios disponíveis no momento do tratamento para que um dado perca a possibilidade de associação com um indivíduo, seja de forma direta ou indireta. Sendo assim, um dado é considerado anonimizado quando depois da utilização de meios técnicos no seu tratamento ele não consiga mais ser associado a seu titular.(PINHEIRO, 2021)

Entendendo as definições, podemos agora entender que a anonimização deve ser vista como um mecanismo de segurança de dados, uma forma a mais de proteger as pessoas que disponibilizaram os dados para o tratamento. Um dado anonimizado não se aplica pela lei como dado pessoal, dessa maneira, o dado anonimizado além de proteger o titular do dado que não pode ser prejudicado, este processo também auxilia a organização a continuar a ter direito sobre os dados, que caso não fossem anonimizados, provavelmente teriam que ser excluídos. Então, a LGPD prevê como algumas situações autorizadas a conservar os dados como em casos de estudos realizados por órgãos de pesquisa, que é recomendado sempre que possível o uso de anonimização, além de também em casos de uso exclusivo pelo controlador com a obrigação do dado estar anonimizado.(PINHEIRO, 2021)

Não existe uma técnica perfeita e única de anonimização, é preciso analisar cada situação que se vê necessário a aplicação de uma técnica de anonimização, para então pensar se será usado algo como supressão, generalização ou outra técnica. O objetivo final é o mesmo independente do método escolhido, é necessário que no final do processo não seja mais possível identificar de maneira direta ou indireta os titulares do dados nem mesmo por quem realizou o processo de anonimização.(BIONI, 2020)

2.7.2 Pseudonimização

Uma maneira de substituir os identificadores dos dados que podem ser usados para relacionar com os titulares destes é o uso da pseudonimização. A utilização deste processo tem como objetivo trocar esses identificadores por pseudônimos ou códigos, de maneira aleatória e independentes das informações anteriores. Porém, este processo ainda permite uma relação desses novos dados com os dados originais, permitindo que seja possível a recuperação das informações iniciais em casos que sejam legítimos e controlados.(PINHO, 2017)

A sua grande utilidade vem nos casos em que a total desconexão dos dados com os titulares não seja viável para o uso no sistema, a empresa pode precisar utilizar algumas dessas informações, mas mantê-las sem nenhum tipo de processamento pode trazer grandes riscos. Porém é importante considerar que apenas o uso de uma pseudonimização não garante que os dados estejam de acordo com as legislações, pois com o auxílio de um conjunto de informações, é possível retornar com as informações de maneira total ou parcial.(PINHO, 2017)

2.7.3 Problemas

Apesar de apontarmos que a anonimização é uma ótima solução para a segurança dos dados, ainda existem alguns problemas. Como apontado por (BIONI, 2020) em seu trabalho, a ideia de que os dados poderiam ser completamente desconectados dos seus titulares, de maneira eficiente e total, entregando um anonimato completo para as pessoas não é totalmente verdade.

Existe uma lógica chamada de "efeito mosaico", em que todo dado que foi anonimizado poderia correr o risco de voltar a ser um dado pessoal, utilizando a agregação de diversos pedaços de informação, que no final poderiam formar novamente o dado pessoal que foi processado. Assim, legislações como a LGPD procuraram estabelecer um conceito mais amplo sobre o que seria um dado pessoal, pois considerar apenas a definição simples de dado pessoal como apenas um dado sem um identificador direto, poderia trazer problemas. Dessa maneira, podemos enxergar que um dado que foi processado e não tem um identificador com algum titular, não garante que ele possa ser livre de uma "reversão"para o dado original. (BIONI, 2020)

2.7.4 Uso para as organizações

Como foi explicado no capítulo da LGPD deste trabalho, a anonimização pode ser uma ferramenta útil para estar em conformidade com a lei. A questão é que para a segurança de dados ela sozinha não resolve os problemas, mas como uma das ferramentas usadas, ela é importantíssima, podendo proteger os dados sem que eles percam a utilidade para a empresa.

2.8 Técnicas de Anonimização

Depois de entender as definições e conceitos e também seus usos, é importante definirmos os tipos de anonimização existentes. Porém, a proposta deste trabalho nessa seção é de ser um resumo de exemplos, pois poderiam existir variados tipos de abordagens para anonimizar os dados, mas o foco será nos usos mais comuns e usados na pesquisa.

2.8.1 Encobrimento de caracteres

Esta técnica consiste basicamente em trocar ou "cobrir"parte dos caracteres de um dado por outro tipo de caractere que representa um símbolo constante. Este carácter representado por um símbolo poder ser algo como um "*".(OLIVEIRA; MADEIRA; MONTEIRO, 2020)

Por exemplo, podemos coletar um dado de uma base de dados referentes a números de telefone de clientes, que seria algo como "91234-5678". Para anonimizar este dado com a técnica desta seção, poderíamos modificar-lo para este formato: "*****-**78". Assim o dono

deste dado poderia reconhecer a própria informação, mas quem não soubesse previamente o dado completo não teria como saber o restante da informação. Abaixo está um exemplo desta técnica aplicada em um número de telefone e em um e-mail.

Tabela 2 – Exemplos de Encobrimento de Caracteres

Pré-Anonimizado	Pós-Anonimizado
55 41 91234-5678	** ** *****-**78
contato@gmail.com	*****to@gmail.com

Fonte: Autoria própria.

2.8.2 Substituição

Uma solução existente para auxiliar na anonimização é a de substituir os dados. Nessa técnica é possível substituir parte dos dados, que possam ser usados para identificar um indivíduo, por algo que não está diretamente ligado a este indivíduo. Podemos pegar como exemplo a substituição de um dado sensível como nome e cpf de uma pessoa, e substituir por um código identificador, dessa maneira não saberíamos ao certo quem seria o titular daqueles dados relacionados com este código, mas ainda teríamos outras informações que podem ser relevantes pro sistema.(CAPARROZ, 2016) Abaixo está um exemplo de aplicação de substituição no nome de dois usuários.

Tabela 3 – Exemplos de Substituição

Pré-Anonimizado	Pós-Anonimizado
Gabriel Barbosa	10001
Pedro Guilherme	10002

Fonte: Autoria própria.

2.8.3 Supressão de atributos

Este caso é mais adequado quando não foi possível usar uma técnica de anonimização eficiente ou quando nem todos os dados sensíveis relacionados são realmente importantes para o uso do sistema no banco de dados. Assim, a supressão de dados ou de atributos consiste em remover uma seção do banco de dados que seja essencial para o sistema. Está técnica pode ser vista como uma maneira de reduzir a quantidade de dados armazenados no banco de dados, diminuindo o risco de vazamento de dados sensíveis ou um uso indevido destes.(OLIVEIRA; MADEIRA; MONTEIRO, 2020)

Podemos pegar como exemplo um banco de dados que possuísse um determinado número de colunas e que uma destas colunas não tivesse relevância na estratégia de negócio da empresa. Assim, para que não houvesse problemas a escolha de remover umas destas colunas do banco de dados seria a melhor escolha. Abaixo temos o exemplo desta técnica

aplicada, sendo a primeira tabela a original e a segunda a tabela após a aplicação da supressão de atributos.

Tabela 4 – Exemplos de tabela antes da Supressão de Atributos

Nome	Telefone	CPF	E-Mail
Gabriel Barbosa	55 41 91234-5678	123.456.789-12	contato@gmail.com
Pedro Guilherme	55 41 98765-4321	321.654.987-12	contato2@gmail.com

Fonte: Autoria própria.

Tabela 5 – Exemplos de tabela depois da Supressão de Atributos

Nome	Telefone	E-Mail
Gabriel Barbosa	55 41 91234-5678	contato@gmail.com
Pedro Guilherme	55 41 98765-4321	contato2@gmail.com

Fonte: Autoria própria.

2.8.4 Generalização

A proposta desta técnica é ser usada em casos em que a informação do dado não precisa ser exata, mas ela ainda pode ter utilidade dentro do sistema da empresa. Assim a generalização ou recodificação visa reduzir a precisão dos dados, tornando eles mais gerais.(BARRETO; HENRIQUE, 2021)

Um exemplo prático disso seria reduzir o dado de "tempo de experiencia", relacionado com a vivência de um profissional com uma determinada linguagem de programação. Assim poderia transformar um dado como "2 anos e 5 meses"de experiência com a linguagem Java e transformá-la em "Entre 1 a 3 anos"de experiência. Abaixo está um exemplo da aplicação da generalização de dados.

Tabela 6 – Exemplos de Generalização

Tipo	Pré-Anonimizados	Pós-Anonimizados
Anos de experiência	3 anos e 4 meses	Entre 1 e 5 Anos
Renda	R$ 8.500	Entre R$ 5.000 e R$10.000

Fonte: Autoria própria.

2.8.5 Perturbação

A técnica de perturbação de dados tem como objetivo também alterar o valor dos dados, semelhante a prática de generalização. Porém, diferente da prática anterior os dados não irão somente perder sua precisão real, eles serão alterados o suficiente para que não seja claro o valor original mas ainda traga uma utilidade real para o sistema, sendo possível aplicar essa técnica de maneira parcial ou total sobre dados. Um exemplo de perturbação de dados é a

micro-agregação, que traz a ideia de substituir os dados pelas médias dos valores e agregar então dados com valores semelhantes.(CAPARROZ, 2016)

Abaixo está um exemplo da aplicação da perturbação de dados.

Tabela 7 – Exemplos de Perturbação

Renda por Usuário	Pré-Anonimizados	Pós-Anonimizados
Gabriel	R$ 5.000	R$ 5.500
Everton	R$ 6.000	R$ 5.500
Pedro	R$ 7.000	R$ 7.750
Bruno	R$ 8.500	R$ 7.750

Fonte: Autoria própria.

2.8.6 Exemplo Geral das técnicas aplicadas

Para deixar ainda mais claro as possíveis aplicações da anonimização, vamos ter a seguir duas tabelas representando um tabela em um banco de dados, com informações sensíveis de usuários. Depois desta tabela, temos um tabela com seus dados anonimizados com os exemplos de técnicas citadas acima.

Tabela 8 – Tabela de Banco de Dados sem Anonimização

Usuário	CPF	E-mail	Renda	Tempo de Experiência
Gabriel Barbosa	123.456.789-12	gabriel@gmail.com	R$7.250	3 Anos
Everton Ribeiro	321.654.978-31	everton@gmail.com	R$5.750	7 Anos
Pedro Guilherme	123.345.456-78	pedro@outlook.com	R$2.500	2 Ano
Bruno Fernandes	234.345.456-12	bruno@yahoo.com	R$4.500	10 Anos

Fonte: Autoria própria.

Tabela 9 – Tabela de Banco de Dados com Anonimização

Usuário	E-mail	Renda	Tempo de Experiência
1001	*****el@gmail.com	R$6.500	Entre 1 e 3 Anos
1002	*****on@gmail.com	R$6.500	Entre 4 a 7 Anos
1004	***no@yahoo.com	R$3.500	Entre 8 a 10 Anos
1003	***ro@outlook.com	R$3.500	Entre 1 e 3 Anos

Fonte: Autoria própria.

3 TRABALHOS RELACIONADOS

Apesar do tema deste trabalho ser um assunto relativamente recente, já existem diversos trabalhos que se relacionam com este tema. Com relação a trabalho sobre aplicabilidade da LGPD, podemos encontrar livros como o (PINHEIRO, 2021) e o (DONDA, 2020) que falam da LGPD de maneira mais geral e completa, às vezes sem se aprofundar em determinados assuntos mas falando de maneira suficiente sobre cada tema da lei brasileira. Por abordar toda a LGPD, esses dois livros falam também sobre a anonimização, trazendo suas definições e onde podem ser aplicadas, além de falar de casos onde é recomendado o uso e os casos em que é obrigado a anonimização.

Ainda temos um texto como o da autora (LORENZON, 2020) que faz uma análise comparativa direta da nossa lei brasileira com a sua irmã europeia, procurando abranger os principais pilares das duas leis. Por falar de um comparação, ela aborda outros temas como a aparição do DPO mas não fala muito sobre a anonimização e seus conceitos e aplicabilidades.

Na questão de anonimização, o tema já é algo mais antigo e acaba existindo mais textos e trabalhos relacionados, porém, priorizamos procurar e estudar trabalhos que conseguissem relacionar a anonimização de dados com as leis de proteção de dados ou casos mais parecidos dentro do Brasil.

Apesar da busca de trabalhos que falassem sobre anonimização relacionado com a LGPD, temos um texto como o do autor (BIONI, 2020), em que é abordado as definições de anonimização juntamente com dados anonimizado. O interessante deste texto são as boas explicações e exemplo que ele traz, ajudando bem na compreensão destes conceitos.

Temos também o texto dos autores (MACHADO; DONEDA, 2019), que abordam o assunto de anonimização, mas em um contexto de criptografia e anonimato. Além disso, esse texto é interessante pelo exemplo aplicado no Brasil e também da discussão da diferenciação de anonimização e pseudonimização.

Podemos observar o texto do (ALVES, 2021) que tenta trazer um panorama de como a LGPD e a proteção de dados tem relação com a anonimização, além de também trazer quais técnicas são mais comuns mundialmente nesta questão. É interessante também como o texto traz a ideia de que o Brasil ainda não está suficientemente madura nessa discussão, além de trazer uma visão jurídica sobre tudo.

Outro trabalho interessante é o das autoras (REIS; RUARO, 2018) que trazem a anonimização como uma possível solução para um conflito entre a privacidade das informações e o interesse de poder manipular estes dados. Dessa maneira as autoras ainda apresentam uma situação em que foi utilizada essa solução. O trabalho também traz a discussão da relativização do direito fundamental à proteção de dados.

Olhando mais especificamente para as técnicas de anonimização usadas, temos os trabalhos como o do autor (CAPARROZ, 2016) e dos autores (OLIVEIRA; MADEIRA; MONTEIRO, 2020). Eles abordam questões relacionadas diretamente com a anonimização e suas aplica-

ções, falando também da relação com as leis. Temos o trabalho dos autores (SOUSA *et al.*, 2020b) em que eles abordam anonimização e LGPD diretamente, mas ainda com criptografia. O interessante ainda é a comparação de técnicas de anonimização e criptografia que eles trazem para ver o quanto elas conseguem auxiliar a organização a cumprir com o que está previsto na regulamentação.

Mais um trabalho encontrado que fala diretamente da LGPD e anonimização é o trabalho dos autores (JúNIOR; MARTINS, 2021b) que falam como a anonimização tira o impacto das consequências que os dados pessoais poderiam trazer, mas que agora anonimizados a organização não precisa mais se preocupar. Eles falam também de como este assunto é pouco compreendido e como isso traz uma insegurança jurídica por não saber como aplicá-la.

Indo para os trabalhos relacionados com as técnicas de anonimização. Temos exemplos práticos que explicam algumas das técnicas utilizadas no processo de anonimização, como por exemplo: supressão, perturbação, generalização, ocultação e outros. Podemos ver então isso nos trabalhos dos autores (OLIVEIRA; MADEIRA; MONTEIRO, 2020), (BARRETO; HENRIQUE, 2021) e (CAPARROZ, 2016).

4 METODOLOGIA

Este capítulo discorrerá de maneira mais aprofundada sobre os métodos empregados para o desenvolvimento deste trabalho e como foram desenvolvidas essas estratégias.

4.1 Pesquisa teórica do trabalho

Para realizar esta parte do trabalho, era necessário desenvolver um conhecimento das leis de proteção de dados como a LGPD e suas origens, assim entendendo conceitos gerais da lei para poder entender as necessidades relacionadas a Anonimização. Para compreender as leis, foram feitas pesquisas sobre algumas lei anteriores que no final foram utilizadas para exemplificar neste trabalho através das ideias do autor (MAYER-SCÖNBERGER, 1997), depois foram feitas leituras de materiais sobre a GDPR como por exemplo a utilização do livro (VOIGT, 2017) e por fim foram feitas leituras sobre a própria LGPD com o uso de textos e livro como os (PINHEIRO, 2021) e (DONDA, 2020). Além disso, ainda foram feitas pesquisas sobre como as normas ISO trazem seus conceitos de segurança da informação nas ISO 27001, 27002 e 27701.

Posteriormente, foram realizadas pesquisas na área de anonimização, a fim de compreender a parte técnica associada a esse tema. Foram fornecidos exemplos de diferentes técnicas, juntamente com suas respectivas aplicações, a fim de possibilitar a compreensão das maneiras pelas quais essas técnicas podem ser utilizadas. A proposta de investigar tanto as leis e normas relacionadas à anonimização quanto a parte técnica tinha como objetivo fornecer uma base sólida para a compreensão da segunda parte deste estudo.

Para alcançar este objetivo de entendimento destes assuntos, foi utilizado o método de pesquisa exploratória, utilizando diversas ferramentas de busca como por exemplo os portais da *Institute of Electrical and Electronics Engineers* (IEEE) e *Association for Computing Machinery* (ACM). Foram encontrados diversos artigos, livros e trabalhos, sendo que de todos apenas alguns foram selecionados baseando-se na relevância e credibilidade de cada um, além de abordar os assuntos que eram buscados para a realização deste trabalho.

4.1.1 Estudo de Caso

Para alcançar os objetivos deste trabalho, foi escolhida a modalidade de pesquisa de estudo de caso, sendo a CELEPAR o objeto de estudo. A proposta de usar esta situação como um estudo de caso é o de observar como é feito de fato o uso da anonimização dentro da organização. Para realizar este estudo, foi então escolhido o objeto de estudo e a questão a ser observada, foi feita a coleta de dados, feita a análise e interpretação destes dados e por fim uma elaboração de exemplos de boas práticas para a aplicação da anonimização.

Estes passos e delimitações podem ser observados como exemplos no trabalho (VENTURA, 2007), em que é exemplificado o funcionamento de um estudo de caso. Como é dito neste trabalho, não existe um roteiro fixo para realizar um estudo de caso, porém, existem passos e escolhas comuns entre trabalhos com este tipo de modalidade. Sendo assim, é possível observar uma referência de estrutura para realizar este estudo com este pilares.

4.2 Análise prática de exemplos da Anonimização

Este estudo consistiu na análise de exemplos práticos de processos de anonimização implementados em uma empresa pública, sendo a CELEPAR, do estado do Paraná, a empresa selecionada para este propósito. Com o intuito de examinar esse caso, foram elaboradas questões que visavam compreender pontos relevantes para a compreensão final da problemática proposta neste trabalho. Essas perguntas foram realizadas através de uma entrevista, sendo elas respondidas pelo funcionário da CELEPAR. Posteriormente, foi realizada uma entrevista complementar para aprofundar e detalhar as respostas que não foram completamente abordadas.

4.2.1 Escolhas do exemplo

Para realizar este estudo, existem algumas escolhas importantes, como por exemplo qual seria a empresa e o funcionário representante que poderiam estar nesta pesquisa. Na questão da escolha da CELEPAR, um dos motivos foi a facilidade de acesso a algumas informações por ser uma empresa pública. Dentro do setor privado, durante as buscas deste trabalho, foram encontradas dificuldades em achar empresas que estivessem abertas a compartilhar informações para este estudo, levando então este trabalho para uma pesquisa no setor público. Além da questão de setor, com a proximidade de empresas do estado do Paraná e atuação forte em Curitiba, a CELEPAR mostrou-se uma empresa extremamente relevante para a área de informática e com ampla quantidade de serviços relacionados com o cidadão do estado do Paraná.

Depois de conseguir contato dentro da CELEPAR, foi considerado que o encarregado com o cargo de Gerente de Segurança da Informação da CELEPAR poderia ser a pessoa escolhida para a entrevista. Esta escolha se deve também pela ampla visão do processo escolhido que ele poderia possuir, considerando que um programador ou um responsável do banco de dados teria talvez um conhecimento mais específico do processo, mas poderiam não conseguir contribuir com outras partes. Dessa maneira, como o intuito do trabalho é a análise do processo de maneira geral, foi feita então a escolha do Gerente de Segurança da Informação, porém, caso o trabalho se ficasse mais em uma parte técnica e específica do processo, a escolha poderia ser diferente.

4.2.2 Perguntas da entrevista

Para realizar a entrevista, era necessário desenvolver perguntas que contemplassem os principais assuntos do tema. Baseado em pesquisas e reflexões sobre este tema, chegou-se a ideia de que os assuntos mais importantes que eram necessários para a realização deste trabalho eram os: Casos em que a anonimização é usada, meios de utilização da anonimização, *software* desenvolvido ou contratado, outros meios de segurança aplicados e desafios na aplicação deste tema. Assim, as perguntas foram pensadas procurando englobar todos estes temas.

As perguntas desenvolvidas para o formulário para que fosse possível entender a a aplicação, necessidade e segurança dos dados com a anonimização na CELEPAR foram as seguintes:

1. Como a CELEPAR lida com as questões jurídicas relacionadas com o processamento de dados?
2. Em quais casos a anonimização de dados é utilizada na CELEPAR?
3. Qual *software* a CELEPAR usa para anonimizar os dados?
4. Quais técnicas de anonimização de dados são aplicadas? Como a CELEPAR garante a eficiência e segurança destas técnicas?
5. Como a CELEPAR armazena os dados antes e depois de anonimizados? Quais medidas de segurança a CELEPAR adota para proteger os dados?
6. Como a empresa está se adequando às exigências da LGPD em relação à anonimização de dados pessoais? Existem diferenças das aplicações antes e depois da chegada da LGPD?
7. Quais são os desafios encontrados na aplicação da anonimização dos dados da empresa?
8. Qual foi o histórico de desenvolvimento das políticas de segurança da CELEPAR? Englobando anos anteriores até a chegada da LGPD atual.
9. Dentro do uso de anonimização, como é feito a escolha do tipo de mascaramento dos dados? Como a empresa analisa a situação e a sua aplicação?

Estas perguntas desenvolvidas foram realizadas em dois momentos de entrevista, o primeiro momento com a maioria das perguntas e o segundo momento com perguntas extras feitas em uma entrevista complementar. Estas perguntas visam alcançar informações relevantes para este estudo, englobando diversos escopos dentro do recorte escolhido para este trabalho. Então existem perguntas referente às leis e conhecimento jurídicos, também perguntas técnicas

de escolhas e estratégias de negócios e por fim os desafios encontrados nas aplicação destes processos analisados.

Dessa maneira, agora o trabalho tentará explicar o porquê de cada pergunta. O objetivo é explicar quais temas cada pergunta aborda, colocando então o objetivo e a resposta que estava sendo desejada ao abordar estas questões.

Sem estar na ordem em que foram realizadas as perguntas, é possível agrupa-las em pequenos grupos com os assuntos de foco de cada uma. A pergunta 1 e 6, traz um escopo na parte jurídica e a visão da CELEPAR com este tema, procurando englobar em como a empresa tenta se adequar e compreender as questões que envolvem a lei e suas mudanças. Além das leis, a questão 8 vem com o objetivo de entender a visão da CELEPAR com as questões de segurança, sem estar diretamente ligado com legislação, para assim poder observar como foi feita a evolução dessas questões de maneira interna, tentando acessar informações que pudessem ser divulgadas sem problemas de confidencialidade.

Indo para o ponto de vista técnico, temos as perguntas 2, 3, 4, 5 e 9 que tem o objetivo de entender a aplicação na prática. Nestas perguntas são abordadas tanto as questões na anonimização aplicada como: o *software* usado, situações que ela é usada, como eles adaptam as técnicas com a situação e a questões de segurança além da anonimização. Nesses pontos, está a parte do trabalho em que é possível de se utilizar a CELEPAR como um exemplo, entendendo como ela usa esta ferramenta.

Por fim, o último ponto está na questão 7. A estratégia de perguntar sobre os desafios tem como objetivo entender as questões negativas do uso da anonimização, indo da visão técnica até a parte humana do processo, com relação a equipe e experiência dentro do desenvolvimento com uso da ferramenta de anonimização.

Após a coleta das respostas por meio da entrevista, o próximo capítulo deste trabalho apresentará os pontos mais relevantes identificados nesses dados. Com base nesses pontos, o estudo também refletirá sobre a aplicação da anonimização, avaliando o exemplo da CELEPAR como referência para outras empresas, analisando seus desafios e escolhas. Além disso, serão discutidos aspectos relacionados à utilidade da anonimização como uma ferramenta auxiliadora para a segurança de dados e o desenvolvimento de *software*. Sempre observando a influência da LGPD diante dos usos de processamento de dados.

Por fim, as considerações finais consistirão em uma reflexão sobre as informações obtidas e analisadas no capítulo de resultados. Nesse sentido, considerando a importância da segurança de dados, o contexto atual das leis de proteção de dados e os exemplos possíveis a serem explorados, pode-se concluir que as ferramentas relacionadas à segurança de dados têm o potencial de fornecer auxílio valioso a todos os envolvidos.

5 RESULTADOS

Este capítulo irá discutir e desenvolver as questões feitas na entrevista que foram respondidas pelo responsável da CELEPAR que aceitou participar do estudo. Como complemento desta parte do trabalho, no final do documento tem um apêndice que mostra todas as perguntas e suas respectivas respostas de maneira completa e sem alterações, assim, será possível realizar a discussão do capítulo atual e caso seja necessário mais detalhes das respostas, será possível conferir na íntegra os resultados.

Como ponto inicial dos resultados, é importante revelar que o responsável da CELEPAR destacou a presença de uma equipe jurídica que está responsável e interessada em ter os conhecimentos necessários com as questões relacionadas com os tratamentos de dados. Dessa maneira, quando é necessário ter alguma demanda com o tratamento de dados, essa equipe pode ser consultada e pode agregar nas questões de privacidade e segurança. Esta questão foi respondida na primeira pergunta do questionário.

Dessa maneira, a CELEPAR tem total capacidade de estar de acordo com qualquer questão jurídica relacionado a segurança, privacidade e direitos dos dados. Caso exista qualquer tipo de mudança na lei, eles também podem se adaptar rapidamente com auxílio de profissionais capacitados para esse auxílio. Isso é um ponto importantíssimo para qualquer empresa, pois uma possível falta de conhecimento poderia ocasionar em problemas maiores.

Além da pergunta sobre as questões jurídicas, a questão número 8 trás como a CELEPAR lidou com as questões de segurança antes da chegada da LGPD. Atualmente a CELEPAR possui normas técnicas e políticas de privacidade e segurança que foram baseadas na LGPD, que foram elaboradas com o propósito de estabelecer bases e princípios essenciais. Porém, além dessas políticas atuais, antes da LGPD a empresa já possuía algumas normas técnicas que foram e estão sendo aperfeiçoadas quando existe necessidade. Dentre algumas áreas desta norma estão: uso de rede interna, e-mail corporativo e de acesso a internet.

Partindo para uma parte mais técnica, podemos ver na terceira pergunta do questionário qual foi o *software* escolhido pela CELEPAR e o porquê da sua escolha. A escolha desta ferramenta foi feita através de um processo de licitação. Foram definidas então especificações técnicas que eram desejadas pela CELEPAR que poderiam ser atendidas por diversas soluções de mercado, dessa maneira, a ferramenta Delphix foi escolhida por atender todas as questões especificadas e possuir o menor valor. No mercado existem diversas soluções de *software* que realizam este tipo de serviço de maneiras variadas, além da possibilidade de uma organização criar uma solução própria, mas a CELEPAR optou por contratar este serviço.

O responsável da CELEPAR conta na segunda pergunta que em situações como nos processos de desenvolvimento, manutenção e teste de aplicações é quando a ferramenta é usada para a anonimização de dados. Para esses casos, é explicado na resposta da quarta questão que esta ferramenta Delphix permite a criação de réplicas virtuais das bases de dados com as informações anonimizadas, permitindo ainda o acesso on-line das equipes que necessi-

tam destes dados para o desenvolvimento. Antes de aplicar a anonimização para estas réplicas da base de dados, é criado um *rule set* que permite anonimizar todas as tabelas e seus campos ou um subconjunto destes.

Dessa maneira, podemos observar que a situação mais citada no uso de anonimização por parte da CELEPAR, está na proteção dos dados que estão sendo utilizados na produção do *software*. No caso da CELEPAR, a utilização de técnicas para anonimizar os dados em outros casos pode estar sendo limitada por questões técnicas, como por exemplo no caso do uso de anonimização para proteção de um banco de dados, pois como será dito nas próximas perguntas, a quantidade de dados que a empresa possui é maior que a capacidade do *software*.

Analisando a situação de proteção de dados utilizados em ambientes de desenvolvimento, teste e manutenção, podemos observar algumas técnicas que seriam viáveis para auxiliar. A Supressão de dados pode ser útil, enviando e utilizando apenas os campos necessário para o desenvolvimento, a Substituição também ajudaria a não expor as pessoas envolvidas e suas informações sensíveis, a perturbação poderia auxiliar tirando a precisão dos dados é também a generalização que faria um trabalho semelhante de remover a precisão.

Cada técnica não é necessariamente concorrente da outra, podemos ver como complementares. Apesar do responsável da CELEPAR não ter entrado em detalhes com todas as técnicas ou situações possíveis de anonimização, podemos observar essas técnicas citadas como possíveis soluções. A utilização de uma única solução não resolve todo o problema na maioria dos casos, mas um conjunto pode ser bem útil para a proteção de dados.

Partindo para a aplicação direta da ferramenta. Para que exista uma eficiência no uso desta, a CELEPAR possui uma equipe capacitada para a utilização do *software*, funcionando como um suporte técnico. No caso desta equipe, eles possuem diversas atribuições, porém, dentre elas está a administração da base de dados de todos os sistemas e também a administração da ferramenta de anonimização. Além disso, a fabricante da ferramenta também oferece um apoio para o uso do seu produto, segundo as regras definidas dentro do seu contrato.

Ainda analisando a parte da equipe de especialistas, na pergunta de número 9 é descrito como funciona o processo de anonimização de dados por parte da equipe especializada. Neste caso, o responsável da CELEPAR explica que a equipe de desenvolvimento entrega informações sobre a modelagem do sistema que está sendo trabalhado e esta equipe, assim, após analisar o caso ela define de que forma os dados serão anonimizados, de acordo com os campos e tabelas necessário, para então entregar novamente para a equipe de desenvolvimento.

Um ponto importante que foi explicado neste trabalho é de que a anonimização pode ser vista apenas como uma recomendação de ferramenta feita pela LGPD. Obviamente ela já existia antes da LGPD e ela pode auxiliar com as conformidades da lei, mas não é uma solução única e definitiva. Assim, podemos ver na quinta questão que a CELEPAR possui diversos recursos de segurança, como *firewall* de rede e controles de acesso, mas em algumas situações a anonimização dos dados pode ser usada para estar dentro da lei. Como é respondido na sexta questão, os dados que foram submetidos a anonimização e que não possam ser revertidos,

não são considerados dados pessoais para a aplicação da lei. Dessa maneira, a CELEPAR irá usar a anonimização para casos como o uso de dados de produção, para que não exista inconformidades com a lei ou possíveis problemas de segurança e privacidade.

Por fim, a última pergunta da entrevista nos traz a resposta sobre os desafios encontrados na aplicação da anonimização de dados. O responsável da CELEPAR conta que existem desafios relacionados aos profissionais da empresa como o processo de aprendizado e adoção da ferramenta que ocorre de maneira lenta, pois envolve diversas áreas internas da empresa. Nesse caso, preparar equipes para o uso da ferramenta pode gerar alto custo,

Existe também uma resistência por parte das equipes, pois o uso de ferramentas que aplicam a anonimização acabam tornando o processo mais trabalhoso e burocrático, o que pode causar sensação de lentidão no processo. Podemos observar em trabalhos como os (BERNI, 2010) e (VARGAS, 2016) em que tornar burocrático o desenvolvimento de *software* pode ser prejudicial, ainda mais se tratando de uma época em que o desenvolvimento de *software* é altamente influenciado por metodologias ágeis. Porém, a esta questão vai além de só mais processos, está situação está ligada com segurança e leis de proteção de dados, o que torna todo este problema um desafio que precisa ser enfrentado.

Além dos desafios com as equipes, existem também os desafios técnicos e suas limitações. No caso da CELEPAR e seu licenciamento atual, a capacidade de mascaramento dos dados é consideravelmente menor do que a demanda real da empresa, precisando assim de uma possível mudança para o aumento de capacidade técnica, exigindo então uma expansão de licenciamento. Novamente podemos também relacionar esse problema com possíveis custos, no caso da CELEPAR que é uma empresa de grandes proporções, é necessário um grande investimento para bancar estruturas e ferramentas de anonimização que atendam às necessidades da empresa.

Podemos observar a questão de alto custo aparecendo com frequência nos desafios. Neste caso, como já foi dito anteriormente, este custo vai estar relacionado com o tamanho da organização. Uma empresa de menor porte vai ter um custo menor para treinar e contratar especialistas, pois suas necessidades são menores, assim como poderá ter uma ferramenta com capacidades menores que atendam suas necessidades. Porém, mesmo que os gastos sejam proporcionais, ainda pode ser algo que pode ser um desafio para as organizações.

Com estas respostas que foram coletadas do questionário, que podemos observar no apêndice deste trabalho, podemos ter uma ideia de aplicação prática destas questões. Cada organização vai possuir seus desafios e capacidades nas questões de seguranças e leis de privacidade, mas estudar um exemplo real com o escopo da anonimização como o estudo aplicado neste trabalho, podemos realizar uma reflexão sobre este tema e possuir um conhecimento de como aplicar estas informações em trabalhos e situações semelhantes no futuro.

5.0.1 Boas práticas para as empresas

De maneira resumida e direta, após entender como foi a aplicação da anonimização no caso da CELEPAR, o trabalho agora vai compilar algumas boas práticas para as organizações que estejam interessadas na aplicação da anonimização. Estas recomendações partem diretamente dos resultados encontrados neste trabalho, baseando-se nas questões consideradas mais relevantes e nas respostas obtidas.

A primeira recomendação é a do auxílio de especialistas nas questões jurídicas. Com a presença de profissionais que dominam este assunto para o apoio ao desenvolvimento de *software*, é possível evitar diversas inconformidades com a lei, diminuindo a possibilidade de reiniciar processos e sistemas que possam estar com problemas relacionados a lei.

A segunda recomendação está ligada com a escolha do sistema para a anonimização, seja uma solução própria ou de terceiros. Para que seja possível encontrar a solução ideal, é preciso um entendimento de quais processos da organização precisam da anonimização e qual a capacidade da empresa. Assim, é preciso observar se a necessidade vem da proteção do banco de dados da empresa, de maneira parcial ou completa, ou se a necessidade vem da proteção de dados que estão em produção, além de observar a quantidade de dados que a empresa precisa anonimizar. Depois de observar pontos como este, a procura pela solução precisa ser feita com base nestes requisitos, até encontrar algo que atenda as necessidades da empresa e seja viável na questão dos custos de aplicação.

A terceira recomendação é a de utilização de diversas ferramentas de segurança. Como foi dito diversas vezes neste trabalho, a anonimização é útil quando utilizada de maneira complementar e não única. Assim, a organização deve buscar mais ferramentas e estratégias de segurança e privacidade, que possam auxiliar a organização nas suas conformidades com as leis.

A quarta recomendação seria o cuidados com os desafios com as pessoas com relação a solução encontrada. Estes desafios estão ligados a diversos três pontos: Capacitação para o uso da solução, adoção da ferramenta durante o desenvolvimento e o cuidado com a burocratização do processo. O primeiro desafio é o treinamento para que os profissionais consigam utilizar a solução encontrada de maneira eficiente, esta situação pode trazer custos financeiros e de tempo. O segundo desafio é o problema dos funcionários adotarem essa nova solução, o que implica na mudança no desenvolvimento dos processos da empresa. Por fim, o último desafio citado é um conjunto dos dois primeiros, pois para não tornar o processo burocrático e lento, vai ser necessário que os profissionais aprendam a ser eficientes e adotem este novos processos, tornando o trabalho geral mais harmonioso.

Estas recomendações são baseadas no caso estudado, porém, outras organizações podem tirar proveito destes pontos, aplicando de maneira mais rápida e adaptando este pontos aprendidos, que só seriam desenvolvimento com a experiência própria.

6 CONSIDERAÇÕES FINAIS

Partindo para as considerações finais deste trabalho, é importante entender novamente os objetivos deste. A ideia de usar um exemplo prático de como a anonimização é aplicada e seus impactos com a LGPD possui suas limitações. Por conter informações sobre segurança e privacidade, não é possível conseguir informações precisas de qualquer empresa, seja por motivos de inconformidades ou por motivos de segurança de suas aplicações. No caso da CELEPAR foi possível o levantamento de informações relevantes para demonstrar como essas questões podem ser aplicadas em uma empresa ligada ao governo. Caso fosse analisada uma empresa totalmente ligada à iniciativa privada, poderiam existir diferenças nas contratações das ferramentas e talvez até no comprometimento com a lei, mas a análise técnica da aplicação ainda poderia ser bem semelhante.

Outro ponto importante de destacar é o escopo da anonimização de dados com a LGPD. Temas de segurança e privacidade são extremamente amplos e podem evoluir em diversas áreas, então para que fosse possível realizar um trabalho como este, foi necessário escolher um escopo menor para a análise desta problemática de segurança de dados. A escolha da anonimização foi pelo fato da sua importância e de seu possível auxílio na aplicabilidade das conformidades com a LGPD, tornando então este escopo em um tema interessante de se observar.

Além disso, é importante falar sobre o momento da recém chegada da LGPD e de que não começou de fato o momento pós-LGPD de fato. Pois o Brasil ainda não vive um momento em que a lei está totalmente difundida, além de que ela está sujeita a diversas alterações, como é visto na comparação da primeira versão da lei em 2018 e nas mudanças que já foram feitas até o ano de 2023 (BRASIL, 2019). Porém, ainda sim é importante observar desde agora como tem sido aplicado às exigências nesse momento de transição, para ser possível ver a evolução da lei e das organizações.

Uma empresa como a CELEPAR sempre teve a necessidade de lidar com normas e políticas de segurança mesmo antes da chegada da LGPD. É interessante observar como a empresa soube se adaptar às mudanças da lei e a evolução das ferramentas e estratégias de segurança e privacidade, porém, para uma análise mais profunda seria necessário outro estudo ainda mais específico, pois políticas de normas são um tema bem abrangente.

Novamente é importante ressaltar a ideia de que a anonimização não é uma solução única e definitiva, mas sim uma ferramenta útil para a segurança de dados. Dessa maneira, é necessário analisá-la como tal, entendendo suas limitações e utilizando diversos outros recursos para que exista uma conformidade com a lei e uma segurança mais completa. Usando o exemplo prático da CELEPAR mostrado nesse trabalho, é visível o uso de mascaramento dos dados para auxiliar em processos como o de produção de softwares que necessitam de acesso aos dados, mas isso não anulou o uso de diversas outras ferramentas.

A presença de uma equipe especializada tanto para o uso de um software específico e também nas questões jurídicas, se mostrou um ponto importantíssimo para o sucesso de casos com o tema deste trabalho. É visível então a importância da capacitação das equipes, já que o pleno conhecimento da lei pode prevenir problemas futuros com relação à privacidade e também o conhecimento de ferramentas e técnicas traz eficiência no desenvolvimento.

Existem também as dificuldades encontradas na aplicação da anonimização durante os processos que necessitam do uso de dados. Foi possível observar esses desafios no capítulo de resultados, envolvendo desde a capacitação e aceitação por parte das equipes, custos técnicos e de treinamento e até as possíveis limitações técnicas que os softwares relacionados a isso podem possuir. Porém, mesmo que seja necessário um treinamento mais sofisticado ou a adição de mais processos burocráticos que diminuam o ritmo nas produções, ainda assim a utilização destas técnicas de anonimização podem auxiliar as organizações em uma maior conformidade com a lei e ainda possuírem informações valiosas que auxiliem as suas estratégias de negócios.

Assim, é possível considerar que o caso da CELEPAR pode ser um bom exemplo de aplicação da anonimização. Existe o fator da confidencialidade que não permite um acesso a todos as informações possíveis relacionadas a segurança, mas com as informações deste trabalho é possível ter uma ideia de como se aplicar. Desde a criação de equipes, escolha ou criação de software para esta ferramenta e de desafios que possam aparecer em organizações que possuem situações parecidas.

Para as boas práticas citadas neste trabalho, apesar delas estarem muito relacionadas com o caso estudo, a proposta não é que seja uma lista rígida, mas sim um exemplo de boas ações que possam auxiliar organizações. Cada empresa tem suas realidades, mas com o auxílio de uma base, é possível se estruturar e se preparar para a aplicação de um caso parecido com base nas boas práticas citadas.

Temas relacionados com segurança da informação, privacidade e leis devem ser cada vez mais difundidos. Ainda existem temas como estes que são muito recentes e não possuem grandes fontes de informação, então por mais que sejam escopos pequenos em trabalhos com temas relacionados, ainda sim é importantíssimo a presença de estudos técnicos e reflexões para que existam evoluções dentro da área.

REFERÊNCIAS

ALVES, D. V. Técnicas de anonimização de dados pessoais e a lei n. 13.709/2018. 2021.

ANDRADE, V. M. de; KIM, S. H. J. Possuir a certificação iso/iec 27001:2013 significa estar compliance com a lgpd? e quais as expectativas para a iso/iec 27701:2019? 2019.

BARRETO, F. G.; HENRIQUE, F. G. Lei geral de proteÇÃo de dados e a aplicabilidade na anonimizaÇÃo. **IV Workshop de Tecnologia da Fatec Ribeirão Preto – Vol.1 – n.4**, Ribeirão Preto - SP, 2021.

BERNI, J. C. A. Gestão para o processo de desenvolvimento de software científico utilizando uma abordagem ágil e adaptativa na microempresa. Santa Maria - RS, 2010. Disponível em: http://repositorio.ufsm.br/handle/1/8132.

BIONI, B. R. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**, v. 53, p. 191–201, 2020.

BOMFIM, L. H. da S. Um servi co para anonimiza c ao em redes definidas por software. Programa de pós graduação em Ciência da Computação/UFS, São Cristóvão, Sergipe, Brasil, 2017.

BRASIL. Lei nº 13.853, de 2019. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

BURILLE, J. R. P. A proteÇÃo de dados pessoais amparada pela lgpd: Um estudo sobre os impactos causados no marketing digital. Porto Alegre - RS, 2022.

CAPARROZ, R. F. Anonimização e o projeto de lei de proteção de dados pessoais. FACULDADE DE TECNOLOGIA DE AMERICANA, Americana, SP, Brasil, 2016.

CELEPAR. **O que Fazemos**. 2023. Disponível em: https://www.celepar.pr.gov.br/Pagina/O-Que-Fazemos.

CELEPAR. **O que é mascaramento de dados?** 2023. Disponível em: https://www.celepar.pr.gov.br/Pagina/Apresentacao.

DELAGUSTINHI, P. A. Análise de ferramentas de mapeamento de dados. Rio Grande do Sul - RS, 2021.

DONDA, D. **Guia prático de implementação da LGPD**. [*S.l.*]: Editora Labrador, 2020.

DONEDA, D. A proteÇÃo dos dados pessoais como um direito fundamental. Espaço Juridico, 2011.

FAL', O. M. Documentation in the iso/iec 27701 standard. **Cybern Syst Anal 57**, 2021.

GALVAO, J. R. O conceito de "dados pessoais" na lei geral de proteÇÃo de dados e no regulamento europeu sobre a proteÇÃo de dados. **Centro Universitário de Brasília - UniCEUB**, Brasília - DF, 2021.

GDPR. Gdpr - general data protection regulation. 2016. Disponível em: https://gdpr-info.eu/.

JESUS, D. C. de. Proposta de um projeto de conformidade a partir das práticas da iso 27701 para implementação de um programa compliance de proteção de dados à luz da lgpd na universidade de rio verde. Rio Grande do Sul - RS, 2022.

JUNIOR, A. E. de A.; SANTOS, E. M. dos; ALBUQUERQUE, E. S. de. Segurança da informação em um instituto de pesquisa: uma análise utilizando a norma iso/iec 27002:2005. Bahia, 2014.

JúNIOR, J. L. d. M. F.; MARTINS, G. M. ProteÇÃo de dados e anonimizaÇÃo: Perspectivas À luz da lei nº 13.709/2018. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, v. 7, n. 1, p. 376–397, abr. 2021. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/476.

JúNIOR, J. L. de M. F.; MARTINS, G. M. ProteÇÃo de dados e anonimizaÇÃo: Perspectivas À luz da lei nº 13.709/2018. 2021.

LIMA, V. H. Lgpd análise dos impactos da implementação em ambientes corporativos: estudo de caso. **Pontifícia Universidade Católica de Goiás**, Goias - GO, 2020.

LORENZON, L. N. Analise comparada entre regulamentações de dados pessoais no brasil e na união europeia (lgpd e gdpr) e seus respectivos instrumentos de enforcement. 2020.

MACHADO, D.; DONEDA, D. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *In*: ____. [*S.l.*: *s.n.*], 2019. p. 99–125. ISBN 978-85-203-6888-6.

MAGALHãES, P. Requisitos e recomendações para o desenvolvimento e operação de um sgsi – abordagem com iso 27001/27002. **Cibersegurança e Informática Forense, Instituto Politécnico de Leiria**, Leiria, Portugal, 2021.

MATTES ícaro V.; PETRI, S. M.; ROSA, M. M. da. SeguranÇa da informaÇÃo contÁbil: procedimentos para elaboração de uma política de segurança com base na iso 27001 e iso 27002. **Revista Interdisciplinar Científica Aplicada**, Blumenau, SC, 2015.

MAYER-SCÖNBERGER. **General development of data protection in Europe**. [*S.l.*: *s.n.*], 1997.

NEVES, R. D. A. P. Gdpr e lgpd: Estudo comparativo. **Centro Universitário de Brasília - UniCEUB**, Brasília - DF, 2021.

OLIVEIRA, E. de; MADEIRA, H. dos S.; MONTEIRO, P. A. M. A lei geral de proteÇÃo de dados pessoais e a anonimizaÇÃo de dados: Uma aplicaÇÃo da tÉcnica em uma base de dados real. Fatec São Cartano do Sul, São Caetano Do Sul, SP, Brasil, 2020.

PINHEIRO, P. P. **Proteção de Dados Pessoais**. 3. ed. [*S.l.*: *s.n.*], 2021.

PINHO, F. A. S. O. **Anonimização de Bases de Dados Empresariais de Acordo Com a Nova Regulamentação Europeia de Proteção de Dados**. 2017. Dissertação (Mestrado), 2017. AAI30204058.

REIS, F. S. dos; RUARO, R. L. A anonimizaÇÃo dos dados como forma de relativizaÇÃo da proteÇÃo de informaÇÕes sigilosas e a atuaÇÃo fiscalizatÓria dos tribunais de contas. REPATS, 2018.

SOUSA, T. *et al.* Lgpd: Levantamento de técnicas criptográficas e de anonimização para proteção de bases de dados. *In*: **Anais do XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. Porto Alegre, RS, Brasil: SBC, 2020. p. 55–68. ISSN 0000-0000. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/19227.

SOUSA, T. *et al.* Lgpd: Levantamento de técnicas criptográficas e de anonimização para proteção de bases de dados. *In*: **Anais do XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. Porto Alegre, RS, Brasil: SBC, 2020. p. 55–68. ISSN 0000-0000. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/19227.

SOUZA, R. M. de. Implantação de ferramentas e técnicas de segurança da informação em conformidade com as normas iso 27001 e iso 17799. Campinas - SP, 2008. Disponível em: http://repositorio.sis.puc-campinas.edu.br/handle/123456789/15094.

TEFFE, C. S. de; VIOLA, M. Tratamento de dados pessoais na lgpd: Estudo sobre as bases legais. 2020.

VARGAS, L. M. Gerenciamento Ágil de projetos em desenvolvimento de software: Um estudo comparativo sobre a aplicabilidade do scrum em conjunto com pmbok e/ou prince2. **Revista de Gestão e Projetos - GeP**, 2016. Disponível em: https://periodicos.uninove.br/gep/article/view/9651.

VENTURA, M. M. O estudo de caso como modalidade de pesquisa. Rio de Janeiro - RJ, 2007. Disponível em: http://sociedades.cardiol.br/socerj/revista/2007_05/a2007_v20_n05_art10.pdf.

VOIGT, P. **The EU General Data Protection Regulation (GDPR): A Pratical Guide**. [*S.l.*]: Springer, 2017. ISBN 978-3-319-57959-7.

APÊNDICE A – Resultado da Entrevista Realizada

Este apêndice ira trazer todas as perguntas e respostas entregues através da entrevista respondida pelo funcionário da CELEPAR. No Capítulo de resultados temos a explicação e discussão sobre essas respostas, mas para complementar e tirar qualquer duvida e ambiguidade que poderia surgir na discussão dos resultados, as respostas completas e sem alterações vão ser apresentadas a seguir.

A.1 Como a CELEPAR lida com as questões jurídicas relacionados com o tratamento de dados?

Na equipe jurídica da Celepar há advogados com conhecimento profundo de questões de privacidade de dados pessoais. Sempre que surgem dúvidas ou demandas em relação ao tratamento de dados pessoais controlados ou operados pela Companhia, a área jurídica é consultada e nos apoia nas decisões e encaminhamentos necessários.

A.2 Em quais casos a anonimização de dados é utilizada na CELEPAR?

Nos processos de desenvolvimento, manutenção e testes de aplicações.

A.3 Qual software a CELEPAR usa para anonimizar os dados? Por que este software foi escolhido?

Delphix. A contratação se deu por processo licitatório, onde havíamos colocado especificações técnicas que poderiam ser atendidas por diversas soluções de mercado. A Delphix foi a vencedora por ter sido a de menor preço que atendeu todos os requisitos do Edital de Licitação.

A.4 Quais técnicas de anonimização de dados são aplicadas? Como a CELEPAR garante e eficiência e segurança destas técnicas?

A ferramenta Delphix possibilita a criação de réplicas virtuais das bases de dados já mascaradas/anonimizadas e que podem ser acessadas on-line pelas equipes de desenvolvimento. Antes da execução do mascaramento/anonimização, para cada base de dados é criado um "rule set", conjunto de regras que nos possibilitam anonimizar todas as tabelas e campos, ou qualquer subconjunto destes. Há uma equipe de suporte técnico da própria Celepar treinada na utilização da ferramenta, além de termos o apoio direto do Fabricante e da revenda que nos forneceu o software, segundo regras definidas em contrato.

A.5 Como a CELEPAR armazena os dados antes e depois de anonimizados? Quais medidas de segurança a CELEPAR adota para proteger os dados?

Na Celepar há diversos recursos de segurança para proteção das bases de dados, incluindo firewalls de rede, controle de acesso (apenas para as pessoas diretamente envolvidas), e processos formalmente instituídos.

A.6 Como a empresa está se adequando às exigências da LGPD em relação à anonimização de dados pessoais? Existem diferenças das aplicações antes e depois da chegada da LGPD?

Não há exigência na LGPD para utililização de dados anonimizados, que na verdade não são considerados como dados pessoais pela LGPD, conforme consta no artigo 12: "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido". Sempre que podemos, utilizamos anonimização para evitarmos acesso ou uso indevido das informações. Não há diferenças nas aplicações antes e depois da LGPD. O que há agora é um cuidado maior para acesso às bases de dados, para evitarmos inconformidades legais ou incidentes de segurança/privacidade.

A.7 Quais são os desafios encontrados na aplicação da anonimização nos dados da empresa?

Processo lento de aprendizado e de adoção da ferramenta por envolver diversas áreas internas. Resistência das equipes de desenvolvimento para utilização por ser algo um pouco mais trabalhoso e burocrático. Há também limitações no licenciamento atual, mas estamos prevendo expansão de licenciamento até dezembro deste ano. Para bases Oracle, que são o maior volume instalado na CELEPAR, em breve estará sendo adquirido licenciamento para mascaramento/anonimização da própria Oracle (option "data masking").

A.8 Qual foi o histórico de desenvolvimento da políticas de segurança da CELEPAR? Englobando anos anteriores até a chegada da LGPD atual.

Na CELEPAR temos políticas de segurança e privacidade, e também normas técnicas. As políticas (de segurança da informação, de privacidade de dados pessoais e de tratamento de incidentes de privacidade de dados pessoais) foram elaboradas com a vigência da LGPD e

estão disponíveis para consulta no site da companhia. Foram redigidas objetivando definições de bases e princípios fundamentais. Desta forma, esperamos que seus textos sofrerão poucos ajustes no decorrer do tempo.

Por outro lado, temos algumas normas técnicas internas que foram elaboradas bem antes da LGPD e vêm sendo aperfeiçoadas ao longo dos anos (por exemplo, de uso de rede interna, email corporativo, e de acesso a internet; está em elaboração neste momento a de acesso a bases de dados de produção). Estas normas trazem definições e orientações práticas para o dia a dia, sendo revisadas e atualizadas sempre que necessário.

A.9 Dentro do uso de anonimização, como é feito a escolha do tipo de mascaramento dos dados? Como a empresa analisa a situação e a sua aplicação?

Há uma equipe na CELEPAR que, entre outras atribuições, administra as bases de dados de todos os sistemas e também a ferramenta de mascaramento. Esta equipe define, após obter informações sobre a modelagem dos dados com os desenvolvedores, de que forma cada campo de cada tabela da base será mascarado. A ferramenta de mascaramento é então configurada e as bases mascaradas são disponibilizadas aos desenvolvedores para uso, que podem ser utilizadas tanto para o desenvolvimento e testes de novas funcionalidades quanto para correções de erros de código.

Apêndice A

UTFPR UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ	Ministério da Educação **Universidade Tecnológica Federal do Paraná** Pró-Reitoria de Graduação e Educação Profissional Pró-Reitoria de Pesquisa e Pós-Graduação Sistema de Bibliotecas

TERMO DE AUTORIZAÇÃO PARA DIVULGAÇÃO DE INFORMAÇÕES DE EMPRESAS

Empresa: Companhia de Tecnologia da Informação e Comunicação do Paraná - CELEPAR	
CNPJ: 76.545.011/0001-19	Inscrição Estadual:_____
Endereço completo: Rua Mateus Leme 1561, Bom Retiro, Curitiba/PR	
Representante da Empresa: Winfried H. Schumann	
Telefone: (41) 3200-6786	e-mail: winfried@celepar.pr.gov.br

Tipo de produção intelectual: (x) TCC[1] ( ) TCCE[2] ( ) Dissertação ( ) Tese

Título/subtítulo: Exemplo de Anonimização Aplicado em Empresas Publicas Baseado na LGPD

Autor: Samuel Leal Valentin	Código Matrícula: a2023989
Autor:_____	Código Matrícula:_____
Autor:_____	Código Matrícula:_____

Curso/Programa de Pós-graduação: Bacharelado em Sistemas de Informação
Orientador: Leandro Batista de Almeida
Co-orientador:_____

Como representante da empresa acima nominada, declaro que as informações e/ou documentos disponibilizados pela empresa para o trabalho citado:

(X) Podem ser publicados sem restrição.

( ) Possuem restrição parcial por um período[3] de _____ anos, não podendo ser publicadas as seguintes informações e/ou documentos:_____

( ) Possuem restrição total para publicação por um período[3] de _____ anos, pelos seguintes motivos:_____

Winfried H. Schumann Gerente de Segurança da Informação	Curitiba, 30 de junho de 2023

[1] TCC – monografia de Curso de Graduação.
[2] TCCE – monografia de Curso de Especialização.
[3] O período de restrição parcial ou total deste Termo deve ser igual ao período definido em termo específico estabelecido entre a UTFPR e a empresa. A íntegra do resumo e os métodos ficarão disponibilizados.