UNIVERSIDADE FEDERAL DE MINAS GERAIS

INSTITUTO DE CIÊNCIAS BIOLÓGICAS

PROGRAMA DE PÓS-GRADUAÇÃO EM INOVAÇÃO TECNOLÓGICA E PROPRIEDADE INTELECTUAL

Frederico Soares Ribeiro

CONSTRUÇÃO DE UMA STARTUP COM O CONCEITO DE PRIVACY BY DESIGN

UM ESTUDO SOBRE A CONNECT POINT

Belo Horizonte

2022

Frederico Soares Ribeiro

CONSTRUÇÃO DE UMA STARTUP COM O CONCEITO DE PRIVACY BY DESIGN

UM ESTUDO SOBRE A CONNECT POINT

Versão Final

Dissertação apresentada ao Programa de Pós Graduação em Inovação Tecnológica e Propriedade Intelectual da Universidade Federal de Minas Gerais, como requisito parcial à obtenção do título de Mestre em Inovação Tecnológica e Propriedade Intelectual.

Orientador: Prof. Dr. Fabrício Bertini Pasquot Polido

Belo Horizonte

2022

043 Ribeiro, Frederico Soares.
Construção de uma startup com o conceito de Privacy by Design: um estudo sobre a Connect Point [manuscrito] / Frederico Soares Ribeiro. – 2022.
103 f.: il. ; 29,5 cm.

Orientador: Prof. Dr. Fabrício Bertini Pasquot Polido.
Dissertação (mestrado) – Universidade Federal de Minas Gerais, Instituto de Ciências Biológicas. Mestrado Profissional em Inovação Tecnológica e Propriedade Intelectual.

1. Inovação. 2. Start up. 3. Processamento de dados. 4. Conformidade em segurança da informação e comunicações. 5 Proteção de dados pessoais. I. Polido, Fabrício Bertini Pasquot. II. Universidade Federal de Minas Gerais. Instituto de Ciências Biológicas. III. Título.

CDU: 608.5

Ficha catalográfica elaborada pela bibliotecária Fabiane C M Reis – CRB 6 – 2680

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS BIOLÓGICAS
MESTRADO PROFISSIONAL EM INOVAÇÃO TECNOLÓGICA E PROPRIEDADE INTELECTUAL

ATA DA DEFESA DA DISSERTAÇÃO DE MESTRADO Nº 155 DE FREDERICO SOARES RIBEIRO

Às 10:30 horas do dia 23 de junho de 2022, em ambiente virtual, realizou-se a sessão pública para a defesa da Dissertação de Frederico Soares Ribeiro. A presidência da sessão coube ao Prof. Dr. FABRÍCIO BERTINI PASQUOT POLIDO, FACULDADE DE DIREITO/UFMG – ORIENTADOR. Inicialmente o Presidente fez a apresentação da Comissão Examinadora assim constituída: PROF. DR. MARCELO GOMES SPEZIALI, UFOP; PROF. DR. RAONI BARROS BAGNO, ESCOLA DE ENGENHARIA/UFMG; PROF. DR. FRANCISCO VIDAL BARBOSA, FACE/UFMG - SUPLENTE; E Prof. Dr. FABRÍCIO BERTINI PASQUOT POLIDO, FACULDADE DE DIREITO/UFMG – ORIENTADOR. EM Seguida, o candidato fez a apresentação do trabalho que constitui sua Dissertação de Mestrado, intitulada “CONSTRUÇÃO DE UMA STARTUP COM O CONCEITO DE PRIVACY BY DESIGN: UM ESTUDO SOBRE A CONNECT POINT”. Seguiu-se a arguição pelos examinadores e, logo após, a Comissão reuniu-se, sem a presença do candidato e do público e decidiu considerar aprovada a Dissertação de Mestrado. O resultado final foi comunicado publicamente ao candidato pelo Presidente da comissão. Nada mais havendo a tratar, o Presidente encerrou a sessão e lavrou a presente ata que, depois de lida, se aprovada, será assinada pela Comissão Examinadora. Belo Horizonte, 23 de junho de 2022.

Documento assinado eletronicamente por **Raoni Barros Bagno**, **Professor do Magistério Superior**, em 27/06/2022, às 16:54, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Fabricio Bertini Pasquot Polido**, **Professor do Magistério Superior**, em 27/06/2022, às 17:49, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcelo Gomes Speziali**, **Usuário Externo**, em 28/06/2022, às 13:59, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufmg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1550708** e o código CRC **B6E9996C**.

Referência: Processo nº 23072.236648/2022-98 SEI nº 1550708

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS BIOLÓGICAS
MESTRADO PROFISSIONAL EM INOVAÇÃO TECNOLÓGICA E PROPRIEDADE INTELECTUAL

FOLHA DE APROVAÇÃO

"CONSTRUÇÃO DE UMA STARTUP COM O CONCEITO DE PRIVACY BY DESIGN: UM ESTUDO SOBRE A CONNECT POINT"

FREDERICO SOARES RIBEIRO

Dissertação de Mestrado defendida e aprovada, no dia 23 de junho de 2022, pela Banca Examinadora constituída pelos seguintes membros:

PROF. DR. MARCELO GOMES SPEZIALI
UFOP

PROF. DR. RAONI BARROS BAGNO
ESCOLA DE ENGENHARIA/UFMG

PROF. DR. FABRÍCIO BERTINI PASQUOT POLIDO – ORIENTADOR
FACULDADE DE DIREITO/UFMG

Belo Horizonte, 23 de junho de 2022.

Documento assinado eletronicamente por **Raoni Barros Bagno**, **Professor do Magistério Superior**, em 27/06/2022, às 16:52, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Fabricio Bertini Pasquot Polido**, **Professor do Magistério Superior**, em 27/06/2022, às 17:49, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcelo Gomes Speziali**, **Usuário Externo**, em 28/06/2022, às 13:59, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Referência: Processo nº 23072.236648/2022-98 SEI nº 1550705

À minha mulher e ao meu filho pelo respeito ao meu período de afastamento em prol da dedicação necessária para conclusão de minha pesquisa e aos profissionais de tecnologia que lidam diariamente com o desafio da privacidade de dados.

AGRADECIMENTOS

Ao Doutor Luiz Cláudio Melo Costa (Bituca) pelo incentivo para meu ingresso no programa de Mestrado Profissional.

Ao Prof. Doutor Fabrício Bertini Pasquot Polido pelo tempo de acompanhamento nesta jornada, incentivando e viabilizando a expansão de meu interesse pela pesquisa.

Aos profissionais que dedicaram um pouco de seu tempo para contribuir para o resultado desta pesquisa.

“A história nos ensina que uma vez estabelecida a sistemática de vigilância, há grande perigo de que as medidas não retrocedam e que os dados já coletados sejam usados em contextos muito diversos daquele que justificaram inicialmente a sua coleta.” (Ministra Rosa Weber)

RESUMO

Após longa tramitação legislativa, em setembro de 2020 entra em vigor a Lei Geral de Proteção de Dados – LGPD, com o intuito de disciplinar e impor cuidados ao tratamento dos dados que possam identificar de forma direta ou indireta uma pessoa natural, preservando os direitos fundamentais.

A adequação às exigências desta legislação pode se tornar um grande desafio para as empresas, principalmente para as *startups* que possuem recursos financeiros limitados e ao mesmo tempo precisam ser escaláveis.

Numa economia cada vez mais digitalizada, é inegável que muitas empresas possuem dentre seus objetivos o tratamento de dados como meio ou diferencial para a entrega de seus serviços ou produtos e diante deste cenário, os titulares dos dados estão cada vez mais conscientes a respeito da importância da tutela sobre os dados pessoais.

Uma *startup* que atua em conformidade à LGPD e possua uma cultura de privacidade já estabelecida, poderá utilizar esse atributo como atrativo para clientes e investidores, sendo, portanto, inegável a relevância de tal adequação para o sucesso do empreendimento.

Após avaliação de diferentes alternativas para buscar a conformidade com a legislação, várias evidências apontaram o *Privacy by Design* como uma alternativa robusta a ser utilizada pelas *startups*, uma vez que possui forte aderência para novos modelos de negócio e necessita de baixo investimento financeiro.

Esta pesquisa, apresenta um estudo de caso realizado junto à *startup* Connect Point que utilizou a metodologia do *Privacy by Design* para se adaptar a este novo momento relacionado à privacidade de dados, implementando de forma orgânica não somente os controles para a conformidade com a legislação, mas também estabelecendo uma cultura de privacidade robusta capaz de proporcionar eficiência no programa de conformidade da empresa.

Palavras-chaves: Privacy by Design; Startup; Tratamento de Dados; Lei Geral de Proteção de Dados – LGPD; Conformidade.

ABSTRACT

In September 2020, after a long legislative proceeding, General Law for Data Protection - LGPD came into effect, aiming at regulating and enforcing caution on data handling, which could identify a natural person directly or indirectly, safeguarding fundamental right.

Adequacy to legislation requirements may turn become a huge challenge to companies, mainly startups, which have limited financial resources whilst need to be scalable. In an increasingly digital economy, it is irrefutable that many companies have among their goals, data handling as a means or differential to services and goods dispencing and in face of this scenario, data holders are each time more aware concerning the relevance of custody over personal data.

Startups operating in accordance with the regulation (LGPD) and have already set privacy culture, will be able to use such attribute as attractiveness for customers and investors. Therefore, the importance of this adequacy is undeniable for businesses success.

After different alternatives assessments seeking compliance with legislation, several evidences aim at Privacy by Design as strong alternative to be used by startups since it has high adhesion to new business models and need low financial investment.

This research presents a case study carried out with Connect Point startup, that used Privacy by Design approach to adapt itself to this new moment related to data privacy, by organically implementing not only the control for legislation adequacy, but also by establishing a strong privacy culture, capable of providing efficiency in the company compliance program.

Key-words: Privacy by Design; Startup; Data handling; (General Law for Data Protection) Lei Geral de Proteção de Dados – LGPD; Compliance

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS

ADI – Ações Diretas de Inconstitucionalidade

ANPD – Autoridade Nacional de Proteção de Dados

APL – Anteprojeto de Lei

CDC – Código de Defesa do Consumidor

CEO – Chief Executive Officer

CEPD – Comitê Europeu de Proteção de Dados

CF – Constituição Federal

CGI – Comitê Gestor da Internet

CLT – Consolidação das Leis do Trabalho

CNIL – Commission Nationale de l'Informatique et des Libertés

CTO – Chief Technology Officer

CVM – Comissão de Valores Mobiliários

DPA – Data Protection Authorities

DPDC – Departamento de Proteção e Defesa do Consumidor

DPO – Data Protection Officer

FBI – Federal Bureau of Investigation

GDPR – General Data Protection Regulation

IBGE – Instituto Brasileiro de Geografia e Estatística

ICO – Information Commissioner's Office

Idec – Instituto Brasileiro de Defesa do Consumidor

LGPD – Lei Geral de Proteção de Dados

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

PL – Projeto de Lei

PP – Política de Privacidade

PRI – Plano de Respostas a Incidentes

PSI – Política de Segurança da Informação

RIPD – Relatório de Impacto de Proteção de Dados

SA – Sociedade Anônima

SI – Segurança da Informação

STF – Supremo Tribunal Federal

UE – União Europeia

SUMÁRIO

1. INTRODUÇÃO

1.1. Contextualização

Inicialmente, cumpre destacar que o direito ao esquecimento é o direito que um determinado indivíduo possui de não permitir que um fato, ocorrido em determinado momento de sua vida, seja exposto ao público em geral, causando-lhe sofrimento ou transtornos. Além disso, é oportuno mencionar que o direito ao esquecimento também é chamado de “direito de ser deixado em paz” ou o “direito de estar só”. Nos Estados Unidos, o direito ao esquecimento é conhecido como “*the right to be let alone*” e está relacionado intimamente ao direito à privacidade “*right to privacy*”.

Pautada neste princípio, a LGPD, Lei Geral de Proteção de Dados, sancionada em agosto de 2018, tem como objetivo a regulamentação do tratamento dos dados pessoais nas organizações, sejam estas privadas ou não, tratadas tanto por meio físico ou digital. A Lei tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade estabelecendo padrões de segurança e responsabilidades pela manutenção e utilização dos dados de pessoa natural, ou seja, de todos os seus clientes e usuários.

BASAN e JÚNIOR (2020) apontam em seu artigo intitulado como “A proteção de dados pessoais e a concreção do direito ao sossego no mercado de consumo” que a proteção de dados pessoais pode se enquadrar como instrumento para a garantia do sossego das pessoas. O estudo toma como base uma verdadeira releitura do direito de ser deixado em paz, classicamente relacionado ao direito de privacidade, para apontar que, na sociedade atual, as publicidades de consumo são capazes de perturbar as pessoas. Isso porque, a partir dos dados pessoais, como o e-mail, o número de telefone e os aplicativos de comunicação, as empresas promovem ofertas de consumo direcionadas, personalizadas, não solicitadas e importunadoras, de modo constante, assediando o consumidor.

Formatada com base na GDPR, *General Data Protection Regulation*, que passou a ser obrigatória em 25 de maio de 2018 e aplicável a todos os países da União Europeia, a Lei Geral de Proteção de Dados - LGPD entrou em vigor no Brasil em 18 de setembro de 2020 para regulamentar o uso de dados pessoais e garantir a

privacidade das pessoas, porém ainda com muitas incertezas quanto à gestão, sanções e responsabilidades.

A LGPD inaugura uma nova cultura de privacidade e proteção de dados no país, o que demanda a conscientização de toda a sociedade acerca da importância dos dados pessoais e os seus reflexos em direitos fundamentais como a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Segundo LINDEN et al. (2020) com a implantação da GDPR foi possível identificar um significativo aumento das revisões das políticas de privacidade dentro e fora da União Europeia e desta mesma forma, esperamos identificar também, tais avanços com relação à LGPD.

1.1.1. A inovação e o tratamento de dados

O tratamento de dados é sem dúvida uma atividade responsável por diferentes iniciativas de inovação por todo o mundo. Uma pesquisa realizada pela plataforma Consultancy.eu[1] em setembro de 2020, aponta que a demanda por novidades e soluções empresariais criativas só cresce, ao passo que ferramentas de monitoramento e análise de dados se mostram cada vez mais relevantes para modelos de governança corporativa. Esta pesquisa reforça a ideia de que o tratamento de dados é um motor para inovação, entretanto há quem ainda não tenha encontrado a melhor maneira de usá-los para desenvolver e/ou melhorar produtos e serviços aos clientes.

A Lei Geral de Proteção de Dados chega com a missão de orientar as empresas de todo o Brasil sobre como realizar o tratamento de dados de maneira correta e transparente, tendo como base três pilares: finalidade, necessidade e adequação. Saber o verdadeiro objetivo de se tratar um dado, seja coletando, armazenando,

[1] Trata-se de uma plataforma online para a indústria de assessoria e consultoria. O site apresenta as últimas notícias e tendências do setor, acompanha os desenvolvimentos e publicações de empresas de consultoria em mais de 60 indústrias e áreas funcionais além de fornecer uma visão geral das oportunidades de carreira para profissionais interessados em trabalhar em consultoria. A pesquisa citada na ocasião, pode ser acessar por meio do endereço eletrônico: https://www.consultancy.eu/news/4901/data-as-the-foundation-for-digital-innovation-in-financial-services

excluindo ou transferindo, como prevê a lei, vai permitir a uma organização entender melhor quem é o seu consumidor.

Com a LGPD, espera-se a adoção de práticas mais robustas relacionadas à governança de dados, contribuindo para a identificação e clareza daqueles que realmente são estratégicos para a empresa e desta forma fomentar a inovação por meio do melhor entendimento de como gerar valor e conhecimento para novos produtos e negócios.

1.1.2. Cenário identificado

Um estudo realizado pela Fundação Dom Cabral no primeiro semestre de 2021 junto a empresas brasileiras, revelou que 20% das empresas entrevistadas, admitem que não estão ajustadas às novas exigências, 16% estão parcialmente ajustadas e 3% não souberam informar, mesmo cientes das possíveis punições. Dentre aquelas que não estarão adequadas até a data limite de adequação, a amostra utilizada neste levantamento não indicou resultados para análise.

De acordo com o pesquisador Doutor Dalton Sardenberg, um dos idealizadores do estudo juntamente com o Doutor Fernando Santiago, o estudo aponta para a necessidade das empresas terem a condução da alta liderança e dos conselhos de administração nos processos que envolvem o *compliance* com as legislações vigentes, principalmente, em relação àquelas que envolvem riscos e prejudicam a reputação das empresas. “De uma maneira geral, os conselhos conhecem, valorizam e consideram a LGPD como prioridade para as empresas. Na maioria dos casos, falta chamar para si a responsabilidade de cobrar a plena adequação nas empresas que administram”, afirma o pesquisador Dalton.

Observando alguns dados da pesquisa, é possível identificar que as empresas com conselho administrativo tendem a ter uma melhor percepção e envolvimento com as ações para implantação da nova lei do que empresas que têm apenas conselho consultivo.

Conforme representado na figura 1, a pesquisa demonstra que 66% das empresas já nomearam um encarregado pela Proteção dos Dados Pessoais, figura também conhecido como Data Protection Officer (DPO).

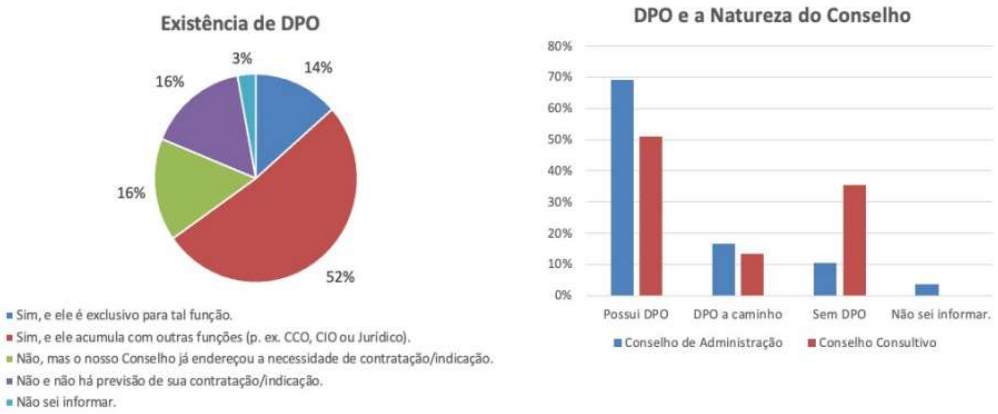


Figura 1 - DPO nas organizações

Fonte: *Sardenberg (2021) – Adaptado pelo autor*

Apesar do conhecimento dos conselhos sobre os impactos da LGPD, a maioria não se considera o maior impulsionador para a adequação, conforme representado pela figura 2.

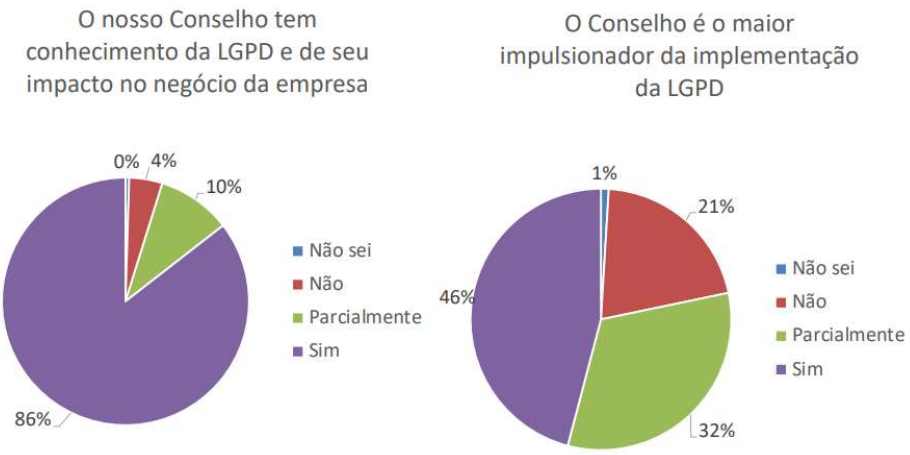


Figura 2 - Visão do Conselho 1

Fonte: *Sardenberg (2021) – Adaptado pelo autor*

61% dos conselhos consideram que a LGPD traz valor para as empresas e não a veem como mais um obstáculo burocrático criado pelo legislador afim de complicar as atividades do empresariado brasileiro, conforme representado pela figura 3.

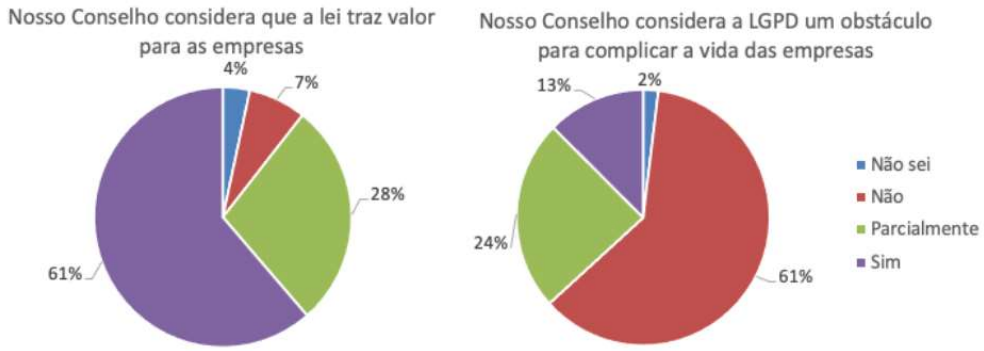


Figura 3 - Visão do Conselho 2

Fonte: *Sardenberg (2021) – Adaptado pelo autor*

Partindo dos resultados observados junto a pesquisa do Professor Doutor Dalton Sardenberg e Professor Doutor Fernando Santiago, é importante buscar alternativas capazes impulsionar o *compliance* junto a empresas mais enxutas, assim como as *startups,* uma vez que muitas vezes não possuem um executivo sênior nem mesmo conselhos administrativos e/ou consultivo.

1.2. Problema de Pesquisa

Embora representantes de *startups* e empresas nascentes reconheçam a importância de se adaptar à LGPD, recursos financeiros limitados e a necessidade de concentrar esforços no modelo de negócio proposto pode influenciar o processo de adaptação deste tipo de empreendimento. Com base neste cenário, como empresas nascentes/*startups* podem se adequar à LGPD a partir de estratégias de desenvolvimento de *Privacy by Design* compatíveis (ou conducentes) com as necessidades de escala, recursos financeiros disponíveis e viabilidade do modelo de negócios que essas empresas objetivam?

1.3. Objetivo

O objetivo principal deste trabalho, é contribuir para que *startups*, empresas de pequeno porte e outras empresas com recursos limitados, possam se adaptar à LGPD de forma gradual e colaborativa entre clientes, fornecedores e funcionários.

1.4. Justificativa

De acordo com o artigo de BREITBARTH (2019) no qual o autor apresenta o cenário da UE após o primeiro ano de vigência da GDPR, observa-se que no período não foi identificada nenhuma redução significativa do quantitativo de vazamentos de dados, mas sim, um aumento das reclamações relacionadas ao *compliance*. Este tipo de reclamação representou quase a metade dos registros junto à DPA - *Data Protection Authorities*, enquanto as violações de dados representavam aproximadamente 1/4 destes registros.

A partir deste artigo, é possível fazer refletir em relação à situação das *startups*, que precisam conquistar a confiança não somente de seus clientes como também dos futuros investidores em um cenário incipiente com relação às regras de privacidade e proteção de dados.

As *startups*, que normalmente são empresas que possuem recursos financeiros mais enxutos, precisam evitar modificações drásticas em seus modelos de negócios, principalmente em função de leis e interferências do governo. Assim, construir o negócio corretamente é também uma forma de economizar dinheiro e tempo para não precisar alterá-lo no futuro. Outro ponto também relevante neste cenário é o fato de que dificilmente uma *startup* receberá um bom aporte de investimento se possuir passivo reputacional perante à sociedade, especialmente no que tange a segurança de dados pessoais.

Conforme definição prevista na LGPD – Lei Geral de Proteção de Dados, os dados pessoais são informações relacionadas à pessoa natural identificada ou identificável e o tratamento de dados consiste em todas operações realizadas com esses dados pessoais, como a utilização, coleta, transmissão, arquivamento, recepção, reprodução, dentre outras ações. Na legislação, toda empresa que faz uso

deste tipo de dados deverá se adequar à LGPD para que o tratamento dos dados seja realizado de acordo com as regras e princípios previstos nesta nova Lei. Adequar à esta nova Lei, não é uma tarefa simples e nem tampouco consiste somente em implementar políticas de privacidade nos meios eletrônicos e investir em segurança cibernética. Embora estas sejam ações que devem fazer parte de uma adequação LGPD, a cultura de privacidade e proteção de dados deve ser implementada na empresa de forma orgânica garantindo uma vigilância constante e preventiva no que diz respeito à prevenção de incidentes.

Na década de 90, Ann Cavoukian, desenvolveu o chamado *Privacy by Design*, que consiste em uma metodologia que prevê a privacidade e a proteção dos dados desde a concepção do produto ou serviço, fazendo com que a proteção dos dados pessoais do titular, que futuramente será o usuário do produto ou serviço, comece a ser pensada no momento de ideação do projeto.

Considerando que as *startups* são empresas que estão no início de suas atividades é essencial que os princípios de privacidade e proteção de dados estejam fortemente atrelados aos seus projetos e para isso a adoção do *Privacy by Design* poderá ser a forma mais rápida e eficiente de atingir uma maturidade em privacidade.

Com o *Privacy by Design* nas *startups*, espera-se evitar problemas que poderão resultar na execução de um novo plano de negócio que possam inviabilizar a implementação do novo produto ou serviço. Este modelo pode ser considerado uma forma de garantir a melhor experiência do usuário já pensando na proteção de seus dados pessoais, como também de assegurar que a *startup* cumpra as diretrizes impostas pela LGPD - Lei Geral de Proteção de Dados desde a sua concepção, reduzindo custos, mitigando riscos e evitando retrabalhos.

Mesmo com a Resolução CD/ANPD nº 2, vale destacar que a dispensa ou flexibilização das obrigações do regulamento "não isenta os agentes de tratamento de pequeno porte do cumprimento dos demais dispositivos da LGPD, inclusive das bases legais e dos princípios, de outras disposições legais, regulamentares ou contratuais relativas à proteção de dados pessoais, bem como direitos dos titulares" (artigo 6º da resolução). Isso significa que, não obstante as poucas flexibilizações, ainda permanece a obrigação de ter um controle sobre as principais tecnologias utilizadas,

os locais de armazenamento dos dados, origem dos dados, compartilhamento com terceiros internos e externos à empresa ou com órgãos públicos, normas claras de retenção e exclusão de dados, além de procedimentos contratuais claros que especificam papéis e responsabilidades de controladores e operadores. Ou seja, as *startups* devem cumprir toda a LGPD, exceto naquilo que foram expressamente dispensadas.

2. REVISÃO BIBLIOGRÁFICA

2.1. Conceituando a privacidade

Considerando a privacidade como o fator mais expressivo em relação à nova legislação, é importante ressaltar que conceituar privacidade trata-se de uma tarefa árdua e com uma amplitude enorme, uma vez que a privacidade consiste na pluralidade de coisas diferentes e que a busca por uma singularidade não resultará no entendimento uma vez que não há uma concepção abrangente como explica SOLOVE (2008).

Muitos reconhecem a importância da privacidade para a liberdade, democracia, bem estar social, bem estar individual e outros fins. O juiz da Suprema Corte Louis Brandeis[2], em 1890 falou da profunda importância de estabelecer e salvaguardar o direito à privacidade, descrevendo tal direito como “o mais abrangente dos direitos e o direito mais valorizado pelos homens civilizados”.

Muito embora a privacidade apresente diferentes concepções sob pontos de vistas acadêmicos e judiciais, é possível estabelecer tópicos de discussões que considerem o direito de ser deixado em paz, o acesso limitado ao eu, o sigilo, o controle de informações pessoais, a personalidade e a intimidade. Estes temas podem se sobrepor, mas cada um deles apresenta uma perspectiva específica sobre a privacidade.

Em 1890, Samuel Warren e Louis Brandeis escreveram seu famoso artigo, “*The Right to Privacy*” aclamado por uma multidão de estudiosos como o fundamento da lei de privacidade nos Estados Unidos. O artigo foi responsável por despertar o interesse a atenção ao tema privacidade, impulsionando a discussão nos Estados Unidos ao longo do século XX.

[2] Apesar de muitos estudiosos admitirem na Common law o reconhecimento jurisprudencial do right of privacy antes do artigo de Warren e Brandeis, o tema não é, entretanto, isento de discussões. De fato, há um grupo considerável de estudiosos que vê nos casos apontados pelo artigo como de reconhecimento do privacy apenas a admissão de outros institutos, como o direito de propriedade, a quebra de contrato, a violação de confiança ou mesmo a ocorrência de difamação, sendo a eventual proteção do privacy apenas incidental. Afirma-se ainda que os argumentos utilizados por Warren e Brandeis para a construção do privacy partiram da errônea compreensão dos precedentes examinados (FESTAS, David de Oliveira. Do conteúdo patrimonial do direito à imagem. p. 156-157).

Warren e Brandeis começaram observando novos desenvolvimentos tecnológicos que representavam uma ameaça potencial à privacidade e se concentraram em como uma lei comum poderia se desenvolver para proteger o interesse então chamado de “privacidade”. Os autores, não dedicaram muitos esforços estabelecendo uma explicação conceitual sobre privacidade e optaram por definir privacidade como o “direito de ser deixado em paz”, frase esta utilizada pelo famoso tratado sobre delitos do juiz Thomas Cooley em 1880[3].

Em 1928, no caso *Olmstead v. Estados Unidos*[4], diante de uma acusação que girava em torno de Washington Roy Olmstead tentar vender bebidas alcóolicas durante o período de Lei Seca, o governo reuniu evidências grampeando os telefones do escritório de Olmstead sem primeiro obter um mandado. Olmstead argumentou que a polícia havia violado os direitos previstos pela Quarta e Quinta Emendas da constituição dos Estados Unidos, entretanto a Suprema Corte em uma decisão de 5 votos a favor contra 4 votos contrários, decidiu que o governo poderia usar as provas obtidas por meio de escutas telefônicas uma vez que não era uma invasão física na casa.

Discordante à decisão no caso Olmstead, Brandeis disparou uma dissidência que se tornaria um dos documentos mais importantes para a lei de privacidade da Quarta Emenda, afirmando que os autores da Constituição “conferiram, contra o governo, o direito de ser deixado em paz – o mais abrangente dos direitos e o mais valorizado pelo homem civilizado”. Em sua dissidência, Brandeis escreveu:

> *“Os escritores de nossa constituição se esforçaram para assegurar condições favoráveis, à busca pela felicidade. Eles reconhecerem a importância da natureza espiritual do homem, de seus sentimentos e de seu intelecto. Eles sabiam que apenas parte da dor, do prazer, dos prazeres e satisfações da vida vinham de coisas materiais. Procuravam proteger os*

[3] Thomas M. Cooley, Law of Torts (2ª ed. 1888). Na mesma época em que Warren e Brandeis publicaram seu artigo, a Suprema Corte se referiu ao direito de ser deixado em paz ao sustentar que um tribunal não poderia exigir que um demandante em um processo civil se submeta a um exame cirúrgico: “Como bem disse o juiz Cooley: 'Pode-se dizer que o direito à própria pessoa é um direito de imunidade completa; ser deixado em paz.'” Union Pac. Ry. Co. v. Botsford, 141 US 250, 251 (1891).

[4] "Olmstead v. United States." Oyez, www.oyez.org/cases/1900-1940/277us438

> *Americanos em suas crenças, seus pensamentos, suas emoções, e suas sensações. Impuseram ao governo o direito de ser deixado em paz - o mais abrangente dos direitos e o mais valorizado pelo homem civilizado."*[5]

O artigo de Brandeis e sua discordância em Olmstead tiveram um impacto profundo na lei de privacidade e nas teorias subsequentes de privacidade. No caso Katz, 1967, a Suprema Corte resolveu rever o pronunciamento adotado em Olmstead, tudo com o propósito de considerar inconstitucional a escuta eletrônica e gravação de conversa entre duas pessoas, ainda que realizada por mecanismos instalados fora da residência dos que sofreram a escuta, de acordo com a redação da Emenda nº 4 à Constituição de Filadélfia.

JOURARD (1966), considera que a concepção de privacidade está relacionada ao segredo, envolvendo apenas o aspecto do acesso ao "eu", considerando a ocultação de fatos pessoais.

O'BRIEN (1979), afirma que a privacidade "pode ser entendida como denotando uma condição existencial de acesso limitado às experiências de vida e compromissos de um indivíduo".

GAVISON (1980), desenvolve a concepção de privacidade como acesso limitado, com o objetivo de definir um conceito neutro de privacidade que seja diferente e coerente, uma vez que as razões pelas quais reivindicamos privacidade em diferentes situações são semelhantes. Segundo a autora, o interesse na privacidade está relacionado à preocupação com a acessibilidade aos outros.

Para POSNER (1981), a privacidade constitui o sigilo à certos assuntos e toda vez que uma informação privada é obtida contra a vontade da pessoa a quem esta informação pertence, caracteriza-se uma violação de privacidade.

INNESS (1992), observa que a privacidade como segredo omite o elemento de controle uma vez que a privacidade pode não necessariamente se opor à publicidade e sua função pode ser fornecer ao indivíduo controle sobre certos aspectos de sua

[5] Tradução realizada pelo autor. Original pode ser acessado em https://caselaw.findlaw.com/us-supreme-court/277/438.html

vida. Esse sentimento também foi reconhecido por BENN (2009) que observou que a privacidade não se refere à assuntos privados que são mantidos fora do conhecimento de outras pessoas que os tornam privados. Em vez disso, os assuntos privados são assuntos sobre os quais seria inapropriado para o conhecimento de outros sem o consentimento do autor.

Uma definição defendida por vários outros estudiosos articulam que a privacidade é a reinvindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como e em que medida as informações sobre eles são comunicadas a outros.

2.1.1. A privacidade frente ao tratamento de dados

O tratamento de grandes bases de dados por mecanismos de processamento muito desenvolvidos pode gerar benefícios até pouco tempo inimagináveis para a sociedade. Esse é o caso, por exemplo, do aplicativo para dispositivos móveis Ginger.io que ao ter acesso a informações extraídas de chamadas telefônicas, mensagens, localização, movimentação e formulários que são preenchidos periodicamente pelo usuário, o mesmo é capaz de prever, por exemplo, que o usuário não está se sentindo bem, ou que está à beira de um ataque de ansiedade. Com uma política de privacidade[6] bastante clara, objetiva e totalmente aderente às leis de privacidade vigente, o aplicativo é o exemplo de como o tratamento de dados por meio de novas tecnologias possibilita a criação de novos produtos e serviços com respeito total à privacidade do indivíduo.

Mesmo que em evidência no cenário de inovação, o tratamento de dados ainda oferece grandes riscos à privacidade, principalmente quando encontramos ambientes de *big data*[7]. No Brasil, a produção de trabalhos acadêmicos ou análises mais

[6] Política de privacidade disponível em https://www.ginger.com/international-privacy, acessado em 01/04/2022.

[7] Big Data é o termo para uma coleção de bases de dados tão grande e complexa que seu processamento se torna difícil se forem utilizadas ferramentas comuns de gerenciamento de bancos de dados ou aplicações de processamento de dados tradicionais. Os desafios incluem a captura, curadoria, armazenamento, pesquisa, compartilhamento, transferência, análise e visualização.

aprofundadas sobre o desafio de se equalizar os direitos à privacidade, a proteção de dados e a inovação ainda se encontram em fase inicial.

Em 15 de abril de 2013, os atletas e expectadores da maratona de Boston, nos EUA, foram vítimas de um ataque terrorista que culminou na morte de três pessoas e dezenas de feridos e o FBI (*Federal Bureau of Investigation*), agência de investigação norte-americana, liderou as investigações para encontrar os responsáveis pelo ataque, conseguindo identificar e capturar os dois suspeitos pelo ataque em menos de 24 horas após a ocorrência do mesmo. O sucesso das investigações somente foi possível por conta da evolução dos mecanismos de coleta e armazenamento de dados, combinada com a alta capacidade de processamento à qual o FBI tinha acesso.

Nos Estados Unidos, é muito comum a prática corporativa de distribuição a consumidores de cupons com descontos sobre produtos. A grande loja de departamento Target decidiu aprimorar essa prática por meio da customização dos cupons com o que ela assumiu serem as preferências de seus clientes. Isso se deu a partir de um software de análise de *Big Data* desenvolvido por um programador da empresa que, reunindo cada uma das compras de cada um dos clientes da Target em todo o território norte-americano em uma grande base de dados, conseguiu identificar uma série de padrões de compras, inclusive aqueles relacionados a pessoas que estavam à espera do nascimento de seus bebês.

Foi após receber um cupom com descontos para artigos de bebês endereçado à sua filha adolescente, um pai se dirigiu indignado à uma das lojas da Target para reclamar que a loja estava induzindo a gravidez de sua filha e encorajando-a a engravidar, o que considerava ser uma prática abusiva por parte da empresa. O gerente que lhe atendeu pediu desculpas e, dias depois, voltou a ligar para o cliente para se desculpar novamente, quando recebeu a resposta de que quem lhe devia desculpas era o pai, já que, ao conversar com sua filha, “tomou conhecimento de algumas atividades que ocorriam em sua casa das quais não tinha ciência”.[8]

[8] FORBES. How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. Disponível em: http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girlwas-pregnant-before-her-father-did, acessado em 02/04/2022.

Ao considerarmos o tratamento de dados pessoais, é importante não nos limitarmos apenas à bancos de dados textuais, mas sim a todo tipo de informação capaz de identificar uma pessoa natural de forma direta ou indireta. Neste sentido, a loja conceito da Hering, a *Hering Experience*, localizada no Morumbi Shopping, em São Paulo, apresentou algumas tecnologias para melhorar o modo de consumo de seus produtos. O estabelecimento instalou câmeras de reconhecimento facial que captavam as reações dos clientes às peças expostas pelo local. Além disso, sensores identificavam quais os locais de preferência do cliente ao circular pela loja. À primeira vista, toda essa tecnologia foi usada para personalizar ofertas e entender o perfil de compra dos clientes, mas o Departamento de Proteção e Defesa do Consumidor (DPDC) classificou essa prática como uma violação à privacidade e instaurou um processo que investiga indícios de coleta de dados dos clientes sem o seu consentimento prévio.

Acreditando se tratar de uma prática que oferece grande risco à privacidade dos clientes que frequentam a loja, o Instituto Brasileiro de Defesa do Consumidor (Idec) realizou a denúncia e em sua defesa, a Hering afirma que diferentemente do que foi apontado, a mesma não realiza reconhecimento facial, mas, sim, detecção facial, por meio do qual estima apenas o gênero, a faixa etária e o humor dos consumidores, de forma anônima. Os argumentos não foram considerados satisfatórios pela Secretaria Nacional do Consumidor que condenou a loja ao pagamento de multa de R$ 58,7 mil por violação ao CDC[9]. Essa foi a primeira condenação no Brasil relativa a violações decorrentes da utilização de tecnologias de reconhecimento facial, amplamente questionada em diversos países.

De acordo com Mark Zukergerg, fundador do Facebook, a privacidade não é mais considerada uma norma social, pois evoluiu com o tempo na medida em que as pessoas têm realmente se sentido mais confortáveis não apenas para compartilhar mais informações e de diferentes tipos, mas também de forma mais aberta e com mais pessoas.[10]

[9] Matéria disponível em https://idec.org.br/noticia/apos-denuncia-do-idec-hering-e-condenada-por-uso-de-reconhecimento-facial, acessado em 03/04/2022.
[10] Matéria disponível em Disponível em: https://www.huffpost.com/entry/facebooks-zuckerberg-the_n_417969, acessado em 03/04/2022.

O discurso do CEO do Facebook, diverge diretamente da visão apresentada por Warren e Brandeis no artigo "*The Right to Privacy*" ademais, o hábito de compartilhar informações e dados pessoais não significa que os indivíduos estão de acordo com o uso indiscriminado desses dados por terceiros, sem seu consentimento ou controle.

2.2. *Privacy by Design*

O conceito de *Privacy by Design* ou "privacidade desde a concepção" consiste em um conceito desenvolvido na década de 1990 pela Dra. Ann Cavoukian, Comissária de Informação e Privacidade de Ontário, no Canadá, para contemplar sua inquietação com os efeitos que poderiam emergir a partir da combinação entre avanço da tecnologia e utilização massiva de dados pessoais pelas empresas. Para ela, o futuro da privacidade não poderia depender apenas de leis e regulações, era preciso incorporar essa preocupação à arquitetura dos sistemas e das funcionalidades, provocando uma mudança nas práticas de negócios, na forma padrão de desenvolvimento, bem como na criação de produtos e serviços pelas empresas.

Em 2009, com a publicação dos 7 principais fundamentos do *Privacy by Design*[11], a Dra. Ann Cavoukian conseguiu consolidar esse conceito e em 2010, com a 32ª Conferência Internacional de Comissários de Privacidade e Autoridade de Proteção de Dados[12], o *Privacy by Design* tornou-se reconhecido como componente essencial da proteção fundamental da privacidade.

O conceito do *Privacy by Design*, está previsto no artigo 25 da *General Data Protection Regulation* - GDPR e também se encontra presente ao longo dos princípios

[11] O artigo com os 7 principais fundamentos do Privacy by Design pode ser acessado por meio do site https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf, acessado em 10/04/2022.
[12] O texto original da resolução que consolida o Privacy by Design como componente essencial para a privacidade pode ser acessado em https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf, acessado em 10/04/2022.

de tratamento de dados previstos pela Lei Geral de Proteção de Dados (LGPD)[13], bem como de forma expressa em seu artigo 46, §2[14].

Os 7 princípios do conceito de "*Privacy by Design*"[15] são representados como:

I. **Proativo e não reativo - ser preventivo e não corretivo**: empresas devem adotar uma abordagem proativa na prevenção de riscos e não na sua remediação.
II. **Privacidade como configuração padrão:** empresas devem projetar seus sistemas, serviços e produtos com proteção automática dos dados pessoais de titulares. O titular não deve ter de realizar ajustes ou tomar providências para garantir a sua privacidade na utilização dos serviços.
III. **Privacidade incorporada ao design**: empresas devem incorporar a proteção de dados pessoais ao design dos seus sistemas e soluções desde a sua formulação mais inicial. Logo, o conceito de privacidade deve constituir uma parte essencial dos serviços e produtos oferecidos.
IV. **Funcionalidade total - soma positiva e não soma igual a zero:** empresas devem evitar "trocas" inadequadas para cumprir com as normas de privacidade. Em outras palavras, deve-se evitar a crença de que é necessário abrir mão da segurança, por exemplo, para coletar mais dados pessoais e atingir os objetivos comerciais do negócio. A equação da privacidade deve ser sempre marcada por um jogo de "ganha-ganha" ("*win-win game*") e não por um jogo de soma zero.
V. **Segurança de ponta a ponta - proteção durante todo o ciclo de vida:** empresas devem implementar medidas de segurança suficientes, desde a formulação do produto ou serviço até o final do ciclo de vida dos dados pessoais.

---

[13] Neste sentido, podem ser citados os princípios previstos no artigo 6º da LGPD, em especial, o princípio da finalidade (I), da adequação (II), da necessidade (III), da transparência (VI), da segurança (VII), da prevenção (VIII), entre outros.

[14] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

[15] Conteúdo original pode ser consultado por meio do endereço eletrônico https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dpd8, acessado em 10/04/2022.

VI. **Visibilidade e transparência:** empresas devem se certificar de que suas práticas comerciais e sistemas operam de acordo com os princípios aplicáveis e sejam verificáveis de forma independente. Além disso, é preciso garantir visibilidade e transparência sobre as finalidades para as quais os dados pessoais dos titulares são processados.
VII. **Respeito pela privacidade do usuário - serviço centrado no usuário:** empresas devem considerar os interesses dos titulares em primeiro lugar no oferecimento de seus produtos ou serviços, garantindo salvaguardas aos seus direitos e liberdades fundamentais.

Em linhas gerais, é pertinente afirmar que o "*Privacy by Design*" representa uma mudança no modo de garantir a privacidade e a proteção de direitos e liberdades dos indivíduos, já que é pensado e incorporado às práticas de negócio antecipadamente, ou seja, desde o momento inicial quando são concebidos os processos produtivos, procedimentos e mecanismos internos do processamento de dados pessoais por Controladores[16], Operadores[17] e terceiros, entretanto, para que isso se concretize na prática, a proteção da privacidade e dos dados pessoais precisa se tornar um valor para a empresa e suas lideranças, a ser disseminado por meio das estruturas de governança e de medidas traçadas nos programas de *compliance*, afim de implementar uma verdadeira cultura de privacidade.

Vale ressaltar, que pensar em *Privacy by Design* deve ser uma das principais metas de empresas que pretendem desenvolver algum produto ou serviço, prezando pela privacidade e pela proteção de dados desde a concepção. Tal conceito permite focar na mitigação do risco desde o desenho inicial do modelo de negócio e este torna-se uma estratégia quando se pretende estar à frente das demais empresas, transmitindo segurança e confiabilidade aos seus usuários e investidores.

Uma segunda abordagem após consolidado o conceito junto à empresa, espera-se a adoção do *Privacy by Default* ou "privacidade por padrão" que consiste na parametrização de que assim que um produto ou serviço for lançado ao público, as configurações mais seguras de privacidade deverão ser aplicadas por padrão, sem

[16] De acordo com o artigo 5º, VI, controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
[17] De acordo com o artigo 5º, VI, operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

nenhuma entrada manual do usuário final. Além disso, todos os dados pessoais fornecidos pelo usuário para permitir o uso ideal de um produto devem ser mantidos apenas pelo tempo necessário para fornecer o produto ou serviço. Se mais informações do que o necessário para fornecer o serviço forem divulgadas, esse conceito será violado. Na prática, um site que utiliza *cookies*[18], eles só podem ser habilitados quando o usuário ativa essa coleta de dados. Caso o visitante de um site não ative os cookies de forma voluntária, não haverá a coleta de informações pessoais do usuário. A Lei Geral de Proteção de Dados exige que todas as empresas que façam o uso dos *cookies* deixem eles desativados por padrão, para o usuário poder decidir quais dados deseja compartilhar.

A privacidade e proteção de dados torna-se parte integrante do desenvolvimento tecnológico e também da maneira de como um produto ou serviço será desenvolvido. Para as empresas que não estão alinhadas com esses conceitos, a LGPD irá provocar uma mudança significativa na cultura, resultando em mais transparência e credibilidade na relação com os clientes.

De modo geral, podemos resumir todo conceito do *Privacy by Design* de acordo com a ilustração a seguir:

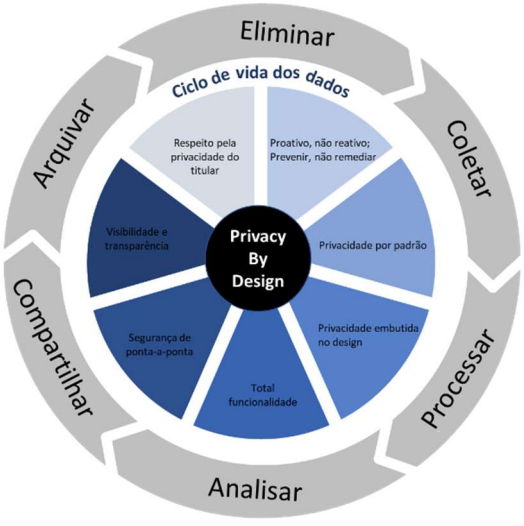


Figura 4 - O Privacy by Design

Fonte: Elaborado pelo autor

[18] Os cookies são um protocolo de pacote de dados que se originou ainda na década de 90, visando garantir a comunicação entre os sites e o usuário final. Pensado como uma solução para o e-commerce, o conceito evoluiu e se tornou presente em todos os tipos de páginas na internet.

O *Privacy by Design* e o *Privacy by Default* estarão presentes em todas as empresas que processam de alguma forma os dados pessoais de seus clientes, colaboradores e fornecedores, sejam estas empresas públicas, privadas, multinacionais ou até mesmo *startups*.

2.3. O Marco Civil da Internet

No que tange à regulação da Internet no Brasil, somente em junho de 2009 o Comitê Gestor da Internet – CGI, editou os Princípios para Governança e Uso da Internet, ou seja, 14 anos após a implementação da rede para uso comercial no Brasil:

> *1. Liberdade, privacidade e direitos humanos: o uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática.*
>
> *2. Governança democrática e colaborativa: a governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva.*
>
> *3. Universalidade: o acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos.*
>
> *4. Diversidade: a diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores.*
>
> *5. Inovação: a governança da Internet deve promover a contínua evolução e ampla difusão de novas tecnologias e modelos de uso e acesso.*
>
> *6. Neutralidade da rede: filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis*

> *motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento.*
>
> *7. Inimputabilidade da rede: o combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos.*
>
> *8. Funcionalidade, segurança e estabilidade: a estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.*
>
> *9. Padronização e interoperabilidade: a Internet deve basear-se em padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento.*
>
> *10. Ambiente legal e regulatório: o ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração. (COMITÊ GESTOR DA INTERNET, 2010)*

Destaca-se entre os princípios acima transcritos o que dispõe sobre o ambiente legal e regulatório para preservar a dinâmica da Internet como espaço de regulação. Em outubro de 2009, a Secretaria de Assuntos Legislativos do Ministério da Justiça, em parceria com a Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, encaminhou o Marco Civil para construção colaborativa para regular utilização da Internet no país, disponibilizando o conteúdo no site do Ministério da Justiça para colaboração de todos que estiverem interessados em colaborar, inclusive via *Twitter*[19], apresentando um claro exemplo do exercício da democracia pelos meios eletrônicos.

Os temas abordados no marco civil incluíram as regras de responsabilidade civil de provedores e usuários sobre o conteúdo postado na Internet e medidas para preservar e regulamentar direitos fundamentais do usuário, como a liberdade de expressão e a privacidade. Neste contexto, ainda foram abordados princípios e

[19] Twitter é uma rede social e um serviço de microblog, que permite aos usuários enviar e receber atualizações pessoais de outros contatos, por meio do website do serviço, por SMS e por softwares específicos de gerenciamento.

diretrizes que com o intuito de garantir algumas das premissas de funcionamento e operacionalidade da rede, como a neutralidade da Internet.

O marco civil não abrangeu de forma aprofundada temas discutidos em outros foros ou que extrapolam a questão da Internet, como direitos autorais, crimes virtuais, comunicação eletrônica de massa e regulamentação de telecomunicações, dentre outros. A proposta de construção do marco regulatório teve como principal objetivo, inovar também no processo de sua formulação: o intuito foi incentivar, através da própria internet, a participação ativa e direita dos inúmeros atores sociais envolvidos no tema e para tanto, o processo foi conduzido, primordialmente, pela própria internet e logo depois encaminhado para apreciação do Congresso Nacional.

Tanto foi o sucesso da participação popular no que tange à regulação da Internet que posteriormente, o próprio Ministério da Justiça se preparou para propor uma lei para proteção dos dados pessoais no Brasil, nos mesmos moldes em que foi feito o marco civil.

2.4. A Lei Geral de Proteção de Dados – LGPD

No âmbito da OCDE, que é composta pelos países mais desenvolvidos, a proteção de dados pessoais ganhou um aspecto maior de discussão a partir da década de 70, com a promulgação da primeira lei sobre o tema no estado de Hesse, na Alemanha Ocidental.

No Brasil, as tratativas para a promulgação de uma legislação abrangente de proteção de dados só começaram a partir de 2010, com a abertura, pelo Ministério da Justiça, da primeira consulta pública do Anteprojeto de Lei (APL) de Proteção de Dados Pessoais[20].

Este APL foi protocolado na Câmara dos Deputados como PL 5.276/2016, de autoria do Poder Executivo, e foi posteriormente apensado ao PL 4.060/12 na data de

[20] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). Tratado de Proteção de Dados Pessoais. 1º ed. Rio de Janeiro: Forense, 2021. pp. 16-17.

18 de julho de 2016[21]. Já em outubro de 2016, foi formada uma Comissão Especial para analisar estes projetos de lei sobre proteção de dados pessoais na Câmara, que realizou ao todo 11 (onze) audiências públicas e um seminário internacional.

Estas tratativas na Câmara também foram acompanhadas por discussões no Senado, até que, no dia 14 de agosto de 2018, foi promulgada a Lei Geral de Proteção de Dados – LGPD, pelo então Presidente Michel Temer a qual dispõe sobre os direitos dos titulares dos dados pessoais e informa como as Empresas e os entes públicos devam tratá-los, sobretudo com regras de *compliance* e alinhadas às boas práticas e governança.

2.4.1. Vigência e sanções

Considerada como uma das leis com *vacatio legis*[22] mais extensos de nossa história, a LGPD entrou em vigor apenas em setembro de 2020, sendo que suas sanções que vão desde bloqueio, exclusão de banco de dados até multa de 2% do faturamento, limitada a R$ 50 milhões reais, entraram em vigor somente à partir de 1º de agosto de 2021.

Nos casos de infrações, para que seja possibilitada a defesa do infrator, serão analisados alguns parâmetros e critérios, como a gravidade e a natureza das infrações e dos direitos pessoais afetados, boa-fé, vantagem competitiva pretendida com a infração, condição econômica, reincidência, avaliação do dano, cooperação com as entidades, e planejamento na adoção das boas práticas de governanças para se adequar à lei.

O artigo 1º da LGPD estabelece as diretrizes básicas da legislação de proteção de dados pessoais, definindo o âmbito de aplicação, a quem se destina e o que visa proteger.

---

[21] A consulta ao PL 5276/2016 está disponível para consulta em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378, acessado em: 01/02/2022

[22] Vacatio legis é uma expressão latina que significa "vacância da lei", ou seja: " A Lei Vaga"; é o prazo legal que uma lei tem pra entrar em vigor, ou seja, de sua publicação até o início de sua vigência.

2.4.2. Abrangência da Lei

Diferentemente do Marco Civil da Internet que teve o objetivo de regulamentar a tratativa de dados somente no ambiente digital, a LGPD se aplica a todas as operações com dados, sejam elas realizadas por meios físicos (arquivos e documentos em papel) ou por meios eletrônicos (bases de dados em ativos informáticos).

A LGPD também se aplica a todas as operações com dados realizadas por quaisquer pessoas físicas ou jurídicas, sejam empresas privadas ou órgãos públicos, e possui a finalidade de proteger a liberdade, a privacidade e os demais direitos fundamentais dos indivíduos em sociedade.

2.4.3. A influência da LGPD

As disposições contidas na LGPD visam elevar o ordenamento jurídico brasileiro ao nível de proteção de dados pessoais visto nos países desenvolvidos, especialmente ao nível de proteção de dados identificados nos países europeus com a GDPR – *General Data Protection Regulation*[23] uma vez que houve o efetivo reconhecimento legal da posição de vulnerabilidade dos indivíduos frente às empresas e governos que se utilizam de seus dados pessoais para os mais variados fins, equilibrando essa relação jurídica[24].

A LGPD apresenta diversos pontos de convergência com a GDPR, fato este explicado pela forte influência da lei europeia na elaboração da lei brasileira. Um destes pontos que se destacam é a maneira que o consentimento se faz veemente resguardado e protegido por ambas as leis. A informação aos titulares dos dados sobre eventuais incidentes, prova do consentimento, portabilidade de dados, indicação e responsabilidade dos agentes encarregados pela operacionalidade dos dados e as regras de segurança para armazenamento, transmissão e manuseio são

[23] DÖHMANN, Indra Spiecker Gen. A proteção de Dados Pessoais sob o Regulamento Geral de Proteção de Dados na União Europeia. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). Tratado de Proteção de Dados Pessoais. 1º ed. Rio de Janeiro: Forense, 2021. pp. 97-98.
[24] COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais – Comentada. 3º ed. São Paulo, Revista dos Tribunais, 2019. pp. 48-49.

pontos essenciais e regulados pela LGPD que constam também no regimento da GDPR.

Apesar de obter mais pontos similares, algumas diferenças se mostram nítidas na comparação entre as duas legislações conforme representado no quadro a seguir:

Tabela 1 - Definições conceituais comparando LGPD e GDPR

Conceito	LGPD	GDPR
Dado Pessoal	Art. 5º, I. Informação relacionada a pessoa natural identificada ou identificável.	Art. 4º - 1) informação relativa a uma pessoa singular identificada ou identificável.
Dado Pessoal Sensível	Art. 5º, II. Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.	Art. 9º - 1) origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.
Titular	Art. 5º, V. Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.	Art. 1º - O presente regulamento estabelece as regras relativas à proteção das pessoas naturais no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
Controlador	Art. 5º, VI. Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.	Art. 4º - 7) a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais.
Operador	Art. 5º, VII. Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlado.	Art. 4º - 8) uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

Encarregado	Art. 5º, VIII. Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).	Art. 39º - "1) O encarregado da proteção de dados tem, pelo menos, as seguintes funções: a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros; b) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do controlador e do operador relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes; c) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35º; d) Coopera com a autoridade de controle; e) Ponto de contacto para a autoridade de proteção de dados".
Tratamento	Art. 5º, X. Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação,	Art. 4º - 2) "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recepção, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou

	transferência, difusão ou extração.	interconexão, a limitação, o apagamento ou a destruição".
Consentimento	Art. 5º, XII. Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.	Art. 4º - 11) "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".
Relatório de Impacto à Proteção de Dados Pessoais (RIPD)	Art. 5º, XVII. Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.	Art. 35º - 1): "1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação".
Autoridade Nacional	Art. 5º, XIX. Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.	Art. 51º - 1) "Os Estados-Membros estabelecem que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do presente regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União. 2. As autoridades de proteção de dados contribuem para a aplicação coerente do presente regulamento em toda a União. Para esse efeito, as autoridades de proteção de dados cooperam entre si e com a Comissão, nos termos do capítulo VII".

Fonte: Elaborado pelo autor

Quando se tratam das bases legais de tratamento de dados, a LGPD apresenta certa inovação em relação à GDPR, quando apresenta 4 bases legais não consideradas pela legislação na qual foi influenciada:

- para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)[25];
- para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)[26];
- para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

2.4.4. Princípios de tratamento de dados

Segundo a LGPD, o tratamento se refere a todas as operações realizadas com dados pessoais, como a coleta, produção, classificação, utilização e transferência dos mesmos. A LGPD, apresenta em seu artigo 6º, princípios relacionados ao tratamento dos dados pessoais de forma à garantir a homogeneidade e a eficácia da norma, a fácil comunicação de seu conteúdo tanto aos titulares quanto aos que realizam o tratamento de dados pessoais, além da compatibilidade com legislações de outros países que utilizem princípios semelhantes.

Nesse sentido, o titular de dados tem a confiança de que as suas informações só serão utilizadas e tratadas em conformidade com as suas expectativas legítimas. Desta forma, o agente de tratamento, a fim de demonstrar a sua boa-fé no tratamento de dados pessoais perante a autoridade reguladora ou autoridade judicial, deverá

[25] Conteúdo pode ser consultado em http://www.planalto.gov.br/ccivil_03/LEIS/L9307.htm
[26] Conteúdo pode ser consultado em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2

pautar suas ações e comprovar através de documentos que está agindo de boa-fé e que está seguindo os princípios elencados pela LGPD.[27]

> *Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
>
> *I – Finalidade: o tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular – não há a possibilidade de tratamento posterior sem que se observem essas finalidades;*
>
> *II – Adequação: o tratamento deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;*
>
> *III – Necessidade: os dados pessoais devem ser tratados respeitando o limite para a realização da sua finalidade, nunca excedendo-a;*
>
> *IV – Livre Acesso: os titulares devem ter garantia para consulta facilitada e gratuita sobre a forma e duração do tratamento, assim como a integridade de seus dados pessoais;*
>
> *V – Qualidade dos dados: os titulares devem ser informados sobre a exatidão, clareza, relevância e atualização de seus dados, de acordo com a necessidade e para o cumprimento da finalidade do tratamento;*
>
> *VI – Transparência: Os titulares devem ter informações claras, precisas e acessíveis sobre o tratamento e seus agentes, observando os segredos comercial e industrial;*
>
> *VII – Segurança: devem ser utilizadas medidas técnicas e administrativas para proteger os dados pessoais de acessos não*

[27] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: o Direito Fundamental à Proteção de Dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). Tratado de Proteção de Dados Pessoais. 1º ed. Rio de Janeiro: Forense, 2021. pp. 39-41.

> *autorizados, acidentes ou situações ilícitas de destruição, perda, alteração, comunicação ou difusão;*
>
> *VIII – Prevenção: devem ser adotadas medidas para prevenir danos decorrentes do tratamento de dados pessoais;*
>
> *IX – Não discriminação: o tratamento de dados pessoais não deve ser utilizado para fins discriminatórios, ilícitos ou abusivos;*
>
> *X – Responsabilização e prestação de contas: o agente deve demonstrar as medidas adotadas e comprovar o cumprimento das normas de proteção de dados pessoais, além de provar a eficácia dessas medidas.*

Com função semelhante ao CEPD (Comitê Europeu de Proteção de Dados) da GDPR, a Autoridade Nacional de Proteção de Dados - ANPD é o órgão da LGPD, vinculado diretamente à presidência da república que fiscalizará os processos de privacidade e proteção de dados realizados pelas empresas, podendo exigir a qualquer momento relatórios de riscos de privacidade.

As empresas devem estar prontas para apresentar termos de uso claros ao usuário, que explicitem quais dados pessoais serão tratados e para qual finalidade. Além disso, elas devem se preparar para atender às solicitações de correção e exclusão de dados, estruturando uma equipe qualificada para realizar esses procedimentos, checagens manuais e o atendimento ao usuário, quando necessário.

2.4.5. A importância da LGPD

É possível comparar o impacto desta legislação no ordenamento jurídico do país à promulgação da Consolidação das Leis do Trabalho (CLT) na década de 40 ou do Código de Defesa do Consumidor (CDC) na década de 90, que também surgiram para equilibrar relações díspares entre as corporações e os indivíduos, conferindo-lhes uma maior proteção legal nas relações de trabalho e nas relações de consumo, respectivamente.

Logo no parágrafo único do artigo 1º, fica evidente que a legislação é de suma importância para o interesse nacional e que deve ser aplicada a todos os entes da federação, entretanto, não prevê a qual ente federativo compete legislar acerca da proteção de dados pessoais. Portanto, ao menos teoricamente, um Estado ou Município poderia legislar de forma supletiva acerca do tratamento de dados pessoais, dando ensejo à criação de complicações ainda maiores para a adequação à legislação por empresas e agentes públicos.

Para sanar esta questão, foi aprovada pelo Congresso Nacional a Proposta de Emenda à Constituição (PEC) nº 17/2019[28], que transfere à União a competência privativa de legislar acerca das questões tratadas na LGPD, conferindo assim uma maior segurança jurídica ao tema.

O artigo 2º da LGPD, lista os fundamentos da proteção de dados pessoais no ordenamento jurídico brasileiro:

> *Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:*
>
> *I - o respeito à privacidade;*
>
> *II - a autodeterminação informativa;*
>
> *III - a liberdade de expressão, de informação, de comunicação e de opinião;*
>
> *IV - a inviolabilidade da intimidade, da honra e da imagem;*
>
> *V - o desenvolvimento econômico e tecnológico e a inovação;*
>
> *VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e*

[28] Esta PEC encontra-se disponível para consulta em https://www25.senado.leg.br/web/atividade/materias/-/materia/135594, acessado em 03/02/2022.

> *VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais*.

Diferentemente dos objetivos contidos no artigo 1º, que se referem a algo exterior a ser perseguido pela legislação[29], os fundamentos criam a base estrutural sobre a qual se forma um sistema legal e de acordo com COMPARATO (2010), o fundamento de algo é a designação do "que serve de base ao ser, ao conhecer, ou ao decidir. Fundamento é, pois, a causa ou razão de algo (*ratio essenci, ratio cognoscendi, ratio decidendi*)".

Considerando o conceito de privacidade já descrito no capítulo 2.1. "Conceituando Privacidade", a privacidade pode constituir uma liberdade negativa, ou seja, um "*direito estático à espera de que seu titular delimite quais fatos da sua vida deveriam ser excluídos do domínio público*", conforme apresentado por BIONI (2020)[30].

Esta liberdade é bastante repercutida diante ao contexto jurídico, seja pelo artigo 12 da Declaração Universal dos Direitos[31], seja pelo inciso X do artigo 5º da Constituição Federal[32] ou pelo artigo 21 do Código Civil[33], estabelecendo-se o trinômio "pessoa-informação-sigilo", devendo qualquer cidadão se abster de adentrar a vida privada de outro cidadão[34], entretanto, últimos anos no qual se viu um aumento exponencial do fluxo de transações com dados pessoais, na chamada era da

---

[29] BASTOS, Celso Ribeiro. Curso de direito constitucional. São Paulo: Saraiva, 2021. pp. 159-1

[30] BIONI. Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2020. p. 118

[31] ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Declaração Universal dos Direitos Humanos, 1949. Artigo 12°: Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.

[32] BRASIL. Constituição da República Federativa do Brasil, 1988. Art. 5º: Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

[33] Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Art. 21: A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

[34] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O Direito Fundamental à Proteção de Dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). Tratado de Proteção de Dados Pessoais. 1º ed. Rio de Janeiro: Forense, 2021. p. 23

informação, o termo “privacidade” ganha uma concepção de liberdade positiva, como uma espécie de proteção dinâmica em relação ao fluxo de informações pessoais disponíveis nos meios tecnológicos, tendo em vista que o próprio acesso a produtos e serviços muitas vezes está condicionado ao fornecimento de dados pessoais.

Um conceito até então pouco utilizado que a LGPD destaca em de extrema importância, é a autodeterminação informativa que significa o poder que cada cidadão tem sobre seus próprios dados pessoais. Isso quer dizer que, em determinadas circunstâncias, ou seja, quando a pessoa puder fazer essa escolha, ela pode decidir se seus dados serão coletados, tratados, compartilhados. A importância da autodeterminação informativa pode ser verificada em um extrato do julgado do tribunal germânico:

> “*aquele que, com segurança suficiente, não pode vislumbrar quais informações pessoais a si relacionadas existem em áreas determinadas de seu meio social, e aquele que não pode estimar em certa medida qual o conhecimento que um possível interlocutor tenha da sua pessoa, pode ter sua liberdade consideravelmente tolhida*”[35].

A LGPD não apresenta novidades ou inovações no tocante propriamente à liberdade de expressão, e sim, vem ratificar a sua importância perante o mundo jurídico e social. O manifestar-se livremente também é assegurado pela lei geral de proteção de dados pessoais este sendo um dos seus fundamentos.

Segundo o artigo 11 do Código Civil, a intimidade, a honra e a imagem são consideradas aspectos irrenunciáveis e intransmissíveis da personalidade. Portanto, neste inciso, a LGPD procurou se adequar à doutrina civilista da dignidade da pessoa humana, buscando proteger todos os aspectos da personalidade contra quaisquer invasões.

Considerando o fato que o tratamento de dados pessoais é a principal ferramenta que viabiliza a transformação digital pela qual a sociedade está passando,

---

[35] MENDES, Laura Schertel. Autodeterminação informacional: origem e desenvolvimento conceitual na jurisprudência da corte constitucional alemã. In: VILLAS BÔAS CUEVA, Ricardo, DONEDA, Danilo, MENDES, Laura Schertel.

a LGPD oferece segurança jurídica a este ambiente de inovação que atrai cada vez mais investimentos ao país, possibilitando que sejam criados e desenvolvidos novos serviços e produtos, utilizando tecnologia de ponta com um arcabouço normativo e regulatório estável.

Desde o surgimento e difusão das redes sociais, já foram vistos diversos casos em que o tratamento de dados pessoais foi utilizado de forma prejudicial aos titulares, em destaque a já evidenciada capacidade de manipulação do comportamento dos indivíduos, retirando-lhes a liberdade de escolha e autodeterminação. É diante de tal potencial que se faz necessária a estruturação de uma legislação para proteção dos dados capaz guiar os futuros reguladores na perseguição do equilíbrio entre as práticas de mercado e a proteção da concorrência.

A influência crescente que o espaço digital vem tendo sobre a vida dos indivíduos em sociedade tem gerado diversas preocupações na temática da proteção dos direitos humanos e neste sentido o Conselho de Direitos Humanos das Nações Unidas publicou disposições para a promoção, proteção e fruição dos direitos humanos no âmbito da internet, destacando que a privacidade do indivíduo é essencial para a efetivação dos direitos à liberdade de expressão, liberdade de opinião e liberdade de associação.[36]

São excluídos da aplicabilidade da LGPD, o tratamento de dados realizado por pessoa natural para fins exclusivamente particulares e não econômicos. Da mesma forma, o emprego de dados pessoais para fins exclusivamente jornalísticos, artísticos e acadêmicos também não precisam seguir as regras estabelecidas na LGPD. Mesmo diante desta não aplicabilidade, qualquer agente que pretender se utilizar desta isenção deverá estar atento à documentação das suas motivações para o enquadramento nesta isenção.

No artigo 46, a LGPD destaca que a segurança de dados deve incluir a garantia de que somente as pessoas devidamente autorizadas e fundamentais podem ter acesso aos dados. Deve-se assegurar também que não haverá tentativas ou situações indevidas e/ou acidentais de perda, alteração, compartilhamento ou

[36] Documento disponível em https://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20, acessado em 04/04/2022

qualquer outro tipo de tratamento com os dados. Para garantir isso, os agentes de tratamento devem tomar medidas técnicas e administrativas.

Os padrões mínimos para esse tipo de proteção poderão ser dispostos pela ANPD, levando em consideração o tipo de tratamento realizado e as possibilidades atuais da tecnologia.

O artigo destaca que esses cuidados devem ser levados em consideração não apenas durante a execução, mas desde a fase de concepção do produto. Isso aproxima a LGPD do conceito de *Privacy by Design,* em que a privacidade e a segurança de dados são parte integrante do desenvolvimento do produto, e não preocupações posteriores.

2.4.6. Proteção de Dados como Direito Fundamental

O Supremo Tribunal Federal decidiu liminarmente, em 07 de maio de 2020, suspender a eficácia da Medida Provisória 954/20[37], que liberava o compartilhamento dos dados dos celulares com o IBGE – Instituto Brasileiro de Geografia e Estatística para que o Governo pudesse enviar mensagens para as pessoas sobre quem estava ou não com COVID.

Isso se deu quando do julgamento das Ações Diretas de Inconstitucionalidade números, ADIs 6.387, 6.388, 6.389, 6.390 e 6.393[38]. Os votos da Ministra Rosa Weber e do Ministro Luiz Fux, já colocavam o direito da proteção de dados como fundamental e seus votos deverão seguir de guia para o Judiciário Brasileiro se posicionar sobre essa matéria.

No dia 10 de fevereiro de 2022, foi aprovada a Emenda Constitucional 115 teve origem na Proposta de Emenda à Constituição (PEC) 17/2019[39]. Tal medida, insere a

[37] Medida Provisória disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm, acessado em 24/03/2022

[38] Documento disponível em https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf, acessado em 24/03/2022

[39] PEC disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757, acessado em 24/03/2022

proteção de dados como direito fundamental na Constituição da República do Brasil, eis o texto:

> *LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022)*
>
> *§ 1º As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata.*
>
> *§ 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.*
>
> *§ 3º Os tratados e convenções internacionais sobre direitos humanos que forem aprovados, em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros, serão equivalentes às emendas constitucionais.*
>
> *§ 4º O Brasil se submete à jurisdição de Tribunal Penal Internacional a cuja criação tenha manifestado adesão.*

Isso significa que, a partir desta data, será assegurado o direito à proteção de dados, inclusive nos meios digitais, no artigo 5º da Constituição Federal e que será de competência privativa da União legislar sobre o tema.

A proteção de dados oficialmente passa a ser um direito autônomo da personalidade, situação que tornará mais segura a sua aplicação e esse direito, apesar de já ter sido reconhecido na decisão histórica do Supremo Tribunal Federal (STF) sobre a Medida Provisória 954/2020 que permitia o compartilhamento de dados pessoais das empresas de telefonia com o Instituto Brasileiro de Geografia e Estatística (IBGE), agora está expresso na Carta Magna e não precisará mais ser extraído de outros direitos constitucionais como a garantia de inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (art. 5º CF).

Este fato, se apresenta como um importante reforço para exaltar que a proteção de dados é coisa séria e deve ser cumprida por toda organização que faça o tratamento de dados pessoais, conforme disposto na LGPD.

2.4.7. A Resolução CD/ANPD nº 2

No último dia 28 de janeiro de 2022, a ANPD – Autoridade Nacional de Proteção de Dados, publicou a Resolução CD/ANPD nº 2[40] que regulamenta o tratamento de dados pessoais por parte de agentes de tratamento de pequeno porte tais como microempresas, empresas de pequeno porte, startups, pessoas jurídicas de direito privado, sociedade limitada unipessoal e microempreendedor individual.

O regulamento de aplicação para agentes de tratamento de pequeno porte visa dispensar ou flexibilizar o cumprimento de algumas obrigações previstas na LGPD para facilitar a operação dos agentes de pequeno porte.

São considerados Agente de Pequeno Porte:

- Microempresas;
- Empresas de pequeno porte;
- Startups;
- Pessoa jurídica de direito privado sem fins lucrativos;
- Pessoas naturais e entes privados despersonalizados, ou seja, que não formalizaram uma empresa, e realizam o tratamento de dados pessoais.

Não se enquadram como agente de pequeno porte:

- Empresas que realizam tratamento de alto risco para os titulares, ressalvada a hipótese de consentimento;
- Empresas com faturamento anual superior à 4,8 milhões de reais (quando microempresa).
- ou superior à 16 milhões no ano calendário anterior (quando startups)

[40] A resolução nº 2 da ANPO está disponível para consulta em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019, acessado em 24/03/2022.

A resolução estabelece critérios classificação do tratamento de alto risco, segmentando os critérios gerais nos quais envolvem tratamento em larga escala ou que possa afetar significativamente interesses e direitos fundamentais dos titulares e os critérios específicos que consideram o uso de tecnologias inovadoras; vigilância ou controle de zonas de acesso público; decisões tomadas com base em tratamento automatizado; utilização de dados sensíveis.

Dentre as obrigações atribuídas aos agentes de pequeno porte, é importante destacar:

- Disponibilizar informações sobre o tratamento e atender as requisições de titulares por meio eletrônico, impresso ou outro;
- Podem se organizar através de entidades de representação para fins de negociação, mediação e conciliação de reclamações apresentadas por titulares;
- Realizar registro de operações de maneira simplificada. A ANPD se compromete a disponibilizar um modelo;
- A comunicação sobre incidentes de segurança também poderá ser realizada de forma simplificada de acordo com disposições da ANPD;
- Os agentes de pequeno porte estão desobrigados da indicação de um DPO, embora esta seja considerada uma boa prática;
- Adotar requisitos mínimos de SI para proteger os dados de acessos não autorizados.

Com relação aos prazos, para os agentes de pequeno porte todos os prazos serão em dobro, a se considerar o que rege na legislação:

- Atendimento aos titulares de dados (ainda será regulamentado);
- Comunicação ao titular e ANPD sobre incidentes de segurança;
- Fornecimento de declaração clara e completa;
- Prazos estabelecidos em normativos próprios para apresentação de informações, documentos, relatórios e registos (caso ainda não tenham sido estipulados prazos a ANPD o fará);
- Fornecer a declaração simplificada no mesmo prazo da completa.

A ANPD enfatiza que levará em consideração as circunstâncias relevantes da situação, natureza da operação, volume e riscos aos titulares para determinar que eventualmente um agente de pequeno porte cumpra as obrigações de forma integral, sem o benefício das flexibilizações permitidas pelo regulamento.

Uma avaliação rápida desta resolução, deixa evidenciado que a Lei apenas passa a flexibilizar alguns pontos em relação a adequação. A flexibilização é vista com bons olhos, uma vez que por exemplo, as empresas de pequeno porte, principalmente as *startups*, são um desafio em relação à necessidade de adequação à Lei, com recursos geralmente limitados. Por outro lado, não se adequar pode facilitar o vazamento de dados, e por consequência, após a crise de um vazamento, pode haver até o fechamento de negócios.

2.5. O Marco Legal das Startups

Em 1º de junho de 2021, entra em vigor a Lei Complementar nº 182/21[41] tratando do Marco Legal das Startups, norma visa estabelecer regramento específico para o setor no país e, assim, fomentar o ambiente de negócios, inclusive quanto à contratação de *startups* pela Administração Pública.

O Marco Legal das Startups apresenta o seguinte conceito:

> *Art. 4º São enquadradas como startups as organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados.*
>
> *§ 1º Para fins de aplicação desta Lei Complementar, são elegíveis para o enquadramento na modalidade de tratamento especial destinada ao fomento de startup o empresário individual, a empresa individual de responsabilidade limitada, as*

[41] Conteúdo completo pode ser acessado em: http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp182.htm#:~:text=LEI%20COMPLEMENTAR%20N%C2%BA%20182%2C%20DE%201%C2%BA%20DE%20JUNHO%20DE%202021&text=Institui%20o%20marco%20legal%20das,14%20de%20dezembro%20de%202006.

> *sociedades empresárias, as sociedades cooperativas e as sociedades simples:*
>
> *I - com receita bruta de até R$ 16.000.000,00 (dezesseis milhões de reais) no ano-calendário anterior ou de R$ 1.333.334,00 (um milhão, trezentos e trinta e três mil trezentos e trinta e quatro reais) multiplicado pelo número de meses de atividade no ano-calendário anterior, quando inferior a 12 (doze) meses, independentemente da forma societária adotada;*
>
> *II - com até 10 (dez) anos de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ) da Secretaria Especial da Receita Federal do Brasil do Ministério da Economia; e*
>
> *III - que atendam a um dos seguintes requisitos, no mínimo:*
>
> *a) declaração em seu ato constitutivo ou alterador e utilização de modelos de negócios inovadores para a geração de produtos ou serviços, nos termos do inciso IV do caput do art. 2º da Lei nº 10.973, de 2 de dezembro de 2004; ou*
>
> *b) enquadramento no regime especial Inova Simples, nos termos do art. 65-A da Lei Complementar nº 123, de 14 de dezembro de 2006.*

Em resumo, a Lei Complementar nº 182/2021, possui 3 escopos que se resumem em:

a) Incentivar o empreendedorismo com soluções inovadoras

Criada a partir de um processo colaborativo entre os poderes Executivo, Legislativo e a sociedade civil, a Lei Complementar nº 182 cria condições facilitadas para empresas com faturamento de até R$ 78 milhões ao ano adotarem a forma societária de Sociedade Anônima fechada. Para isso, ficam autorizadas a realização

das publicações obrigatórias em meio digital e a substituição dos livros físicos por registros eletrônicos.

A legislação também confere à Comissão de Valores Mobiliários (CVM) a possibilidade de dispensar ou modular obrigações para SAs abertas com faturamento de até R$ 500 milhões, com o objetivo de facilitar o acesso ao mercado de capitais. A CVM poderá dispensar ou modular, entre outros, a forma de realização das publicações obrigatórias, a obrigatoriedade de instalação de conselho fiscal e de intermediação de instituição financeira em distribuições públicas de valores mobiliários.

b) Incentivar o poder público à aquisição de soluções inovadoras;

Um dos objetivos da Lei Complementar nº 182/2021 é disciplinar a licitação e a contratação de soluções inovadoras pela Administração Pública, tendo como princípios e diretrizes fundamentais incentivar a contratação de soluções elaboradas ou desenvolvidas por startups. Com a aplicação deste modelo, a força do Estado promete ser utilizada para fomentar a inovação e o uso de tecnologia pelas empresas, e pela própria administração.

c) Criar regras aos contratos com investidores

Com a nova legislação, as startups poderão receber investimentos de pessoas físicas ou jurídicas que não sejam considerados como participação em seu capital social, a depender da modalidade escolhida pelas partes. O investidor que realizar o aporte de capital sem ingressar no capital social não será considerado sócio nem possuirá direito à gerência ou voto na administração da empresa investida. Essa medida afasta a responsabilização do investidor, que não responderá por qualquer dívida da startup, exceto em caso de conduta dolosa, ilícita ou de má-fé por parte do investidor.

2.5.1. Caracterizando uma startup

RIES (2012) caracteriza uma startup como um modelo de empreendedorismo que preza pelo *feedback* contínuo, seja quantitativo ou qualitativo resumindo como um ciclo capaz de construir, medir e aprender. Uma *startup* é muito mais do que um novo produto, uma inovação ou uma ideia brilhante e sim uma iniciativa intensamente humana projetada para enfrentar situações de extrema incerteza.

GITAHY (2011) apresenta que o conceito startup começou a se popularizar na década de 1990 mais especificamente a partir do início da “bolha” da internet nos Estados Unidos. O termo começou a ser difundido no Brasil, entretanto, somente a partir do período compreendido entre 1999 a 2001.

Na visão de LONGHI (2011) *startups* são pequenas empresas montadas em casa ou em faculdades e que recebem pequenos aportes de capital explorando áreas inovadoras, mais comumente de tecnologia, possuindo uma aceleração de crescimento muito alta já nos primeiros meses de existência em virtude de investimentos feitos por fundos de investimento especializados.

HERMANSON (2011), por sua vez, ressalta que startups não são necessariamente somente empresas de tecnologia; mas toda e qualquer empresa em fase de constituição.

Associação Brasileira de Startups, considera que as *startups* são consideradas empresas nascentes de base tecnológica, que possuem na inovação tecnológica disruptiva os fundamentos de sua estratégia competitiva. Entre as principais características de tais negócios está o caráter de organização temporária com potencial de rápido crescimento. Estes negócios atuam em um ambiente de extrema incerteza, em busca de um modelo de negócios que possa tornar-se repetível e escalável.

Os impactos das startups já se refletem no cotidiano da nossa sociedade como se pode observar no sucesso do transporte por aplicativo, *delivery* e outros serviços que utilizam até mesmo as redes sociais. A rápida transformação do mundo nos últimos 30 anos é responsável por grandes transformações no âmbito jurídico também. Por conta disso, verificar como as relações sociais e jurídicas foram afetadas

a partir desse novo modelo de negócio se tornou uma questão necessária e lógica pelos operadores do direito. Chamado de Direito 4.0, as *Legal Startups* de cunho jurídico inovam o jeito de operar o direito. Um exemplo disso é a automação do setor. Softwares de gestão se tornaram ferramentas imprescindíveis para a rotina do profissional do direito que passou a contar com um processo de trabalho eletrônico. Com informatização da justiça, houve uma melhoria na gestão dos processos, trazendo maior organização e eficiência à tradicional área jurídica.

2.6. A relação da LGPD e Marco Legal das Startups

Grande parte do dinamismo e criatividade no desenvolvimento de inovação, está por muitas vezes relacionadas à atuação das *startups*. Toda esta dinâmica criativa, envolve em diferentes esferas, a aplicação de ferramentas que possuem em sua essência a avaliação de cenários e perfis que se baseiam no tratamento de dados. Considerando que de acordo com a Lei Geral de Proteção de Dados, um dado pessoal é toda informação que permita identificar direta ou indiretamente uma pessoa natural, muitas startups estão igualmente obrigadas a buscar a conformidade, mesmo considerando o Normativo nº 02/2022 da ANPD.

Diante desta relação direta entre as startups e o tratamento de dados pessoais, surge um novo desafio que é o de garantir a consolidação dos modelos de negócios dessas empresas, que têm sido chave para o avanço da economia digital, e gerenciar incertezas regulatórias advindas de soluções inovadoras, sem precedente no mercado.

Avaliando a aplicação da LGPD bem como o Marco Legal de Startups, observa-se que ambas proporcionam o espaço para a instituição de *sandboxes*[42] regulatórios para *startups* (e não só essas empresas) que tratam dados pessoais.

[42] O sandbox consiste em um "conjunto de condições especiais simplificadas para que as pessoas jurídicas participantes possam receber autorização temporária dos órgãos ou das entidades com competência de regulamentação setorial para desenvolver modelos de negócios inovadores e testar técnicas e tecnologias experimentais, mediante o cumprimento de critérios e limites previamente estabelecidos pelo órgão ou entidade reguladora e por meio de procedimento facilitado."

O Marco Legal de Startups inova em relação à vários países ao propor um *sandbox* regulatório em lei geral, aplicável a todos os setores regulados, e em âmbito federal.

De acordo com o artigo 55-J, da Lei Geral de Proteção de Dados, compete à ANPD:

> *"XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;"*

Em avalição ao Marco Legal das Startups, também é possível identificarmos este espaço destinado ao incentivo à inovação descrito no artigo 2º, que considera:

> *"II - ambiente regulatório experimental (sandbox regulatório): conjunto de condições especiais simplificadas para que as pessoas jurídicas participantes possam receber autorização temporária dos órgãos ou das entidades com competência de regulamentação setorial para desenvolver modelos de negócios inovadores e testar técnicas e tecnologias experimentais, mediante o cumprimento de critérios e de limites previamente estabelecidos pelo órgão ou entidade reguladora e por meio de procedimento facilitado."*

Considerando os cenários mais comuns, o regulador é sempre quem dita o momento que algo será regulado e quais serão as normativas, entretanto avaliando o conteúdo não somente da LGPD como também do Marco Legal das Startups, é identificado que o mercado pode se posicionar e promover um diálogo para discutir novos modelos de negócio.

Este ambiente regulatório e colaborativo envolvendo um ecossistema cada vez mais evoluído, com o surgimento contínuo de tecnologias disruptivas e que escalam

de forma exponencial deve ser explorado de forma a agregar valor ao negócio e promover a competitividade.

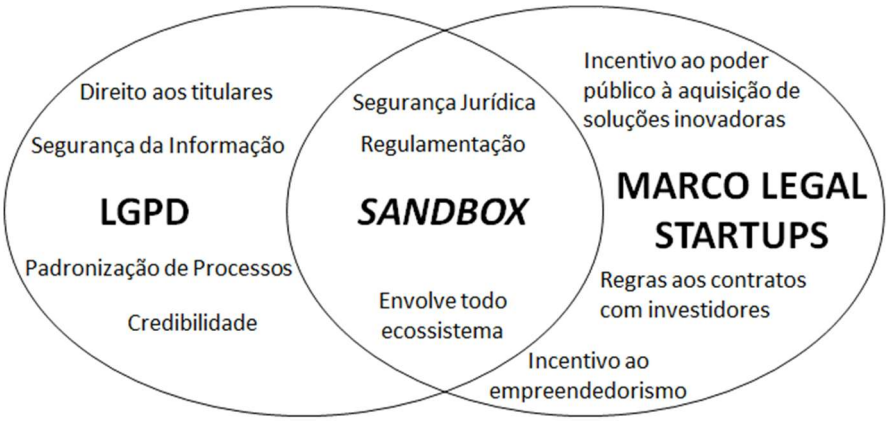


Figura 5 - Relação LGPD x Marco Legal das Startups

Fonte: *Elaborado pelo autor*

A criação de *sandbox* específico para a proteção de dados pessoais no Brasil pode ser objeto de estudo futuros, uma vez que o Brasil se encontra há pouco mais de 1 ano da vigência da LGPD.

3. METODOLOGIA

Nesta pesquisa, foi realizado o que conforme descrito por COOPER e SCHINDLER trata-se de um estudo descritivo, uma vez que conforme os autores, neste modelo de estudo, o "*pesquisador tenta descrever ou definir um assunto, normalmente criando um perfil de um grupo de problemas, pessoas ou eventos*" (COOPER; SCHINDLER, 2003, p. 31).

Esse estudo em questão, utiliza um enfoque qualitativo de pesquisa, baseando-se na descrição e interpretação de fenômenos, com foco na identificação de padrões e comportamentos identificados na *startup* utilizada como objeto de estudo.

A estratégia de pesquisa utilizada foi um estudo de caso único com foco para o entendimento da dinâmica organizacional presente em uma única configuração. De acordo com o artigo "Para que servem os Estudos de Caso Único" (MARIOTTO *et al*., 2011)[43], embora se saiba que nem os estudos de caso único nem os estudos de casos múltiplos permitam generalizações estatísticas, deles podem ser extraídas algumas generalizações analíticas (Chima, 2005; Eisenhardt, 1989; Eisenhardt & Graebner, 2007; Platt, 2007; Yin, 2005). Isto significa dizer que, a partir das observações empíricas, podem ser feitas generalizações para a teoria (a serem posteriormente testadas), e não diretamente para a população (Eisenhardt, 1989; Eisenhardt & Graebner, 2007; Stake, 2000; Yin, 2005).

Segundo YIN (2005), o estudo de caso pode ser tratado como importante estratégia metodológica para a pesquisa em ciências humanas, pois permite ao investigador um aprofundamento em relação ao fenômeno estudado, revelando nuances difíceis de serem enxergadas "a olho nu". Além disso, o estudo de caso favorece uma visão holística sobre os acontecimentos da vida real, destacando-se seu caráter de investigação empírica de fenômenos contemporâneos.

Vale ressaltar, que os resultados apresentados nessa pesquisa, não representam nenhuma generalização estatística dado ao fato de que o caso apresentado não representa uma "unidade de amostragem". Desta forma, fica entendido conforme destacado por YIN (2005), que os estudos de caso individual são

[43] Este artigo está disponível para consulta em http://www.anpad.org.br/admin/pdf/EPQ517.pdf, acessado em 08/04/2022

selecionados da mesma forma que um pesquisador de laboratório seleciona o assunto de um novo experimento.

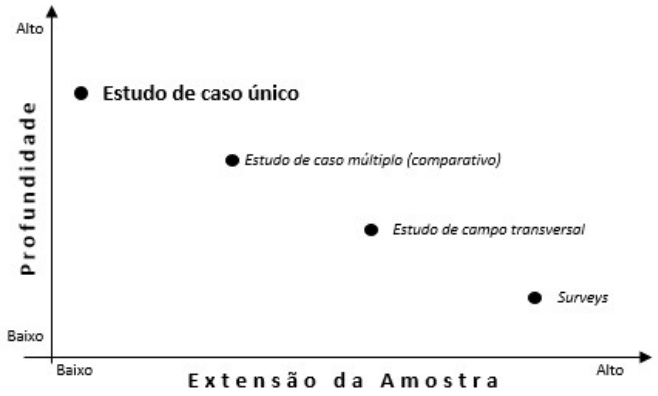


Figura 6 - Características dos estudos de caso

Fonte: Adaptado de Lilis e Mundys, 2005

Yin (2001) e Paré (2004) indicam que uma metodologia para estudos de caso deve ser dividida nas seguintes etapas:

I. Desenho do estudo de caso;
II. Condução do estudo de caso;
III. Análise das evidências do estudo de caso;
IV. Escrita do estudo de caso.

A etapa IV (Escrita do estudo de caso), pode ser realizada de forma paralela com as etapas II (Condução do estudo de caso) e III (Análise das evidências do estudo de caso) se assim preferir o pesquisador. Este roteiro pode ser representado conforme figura 7 apresentada a seguir:

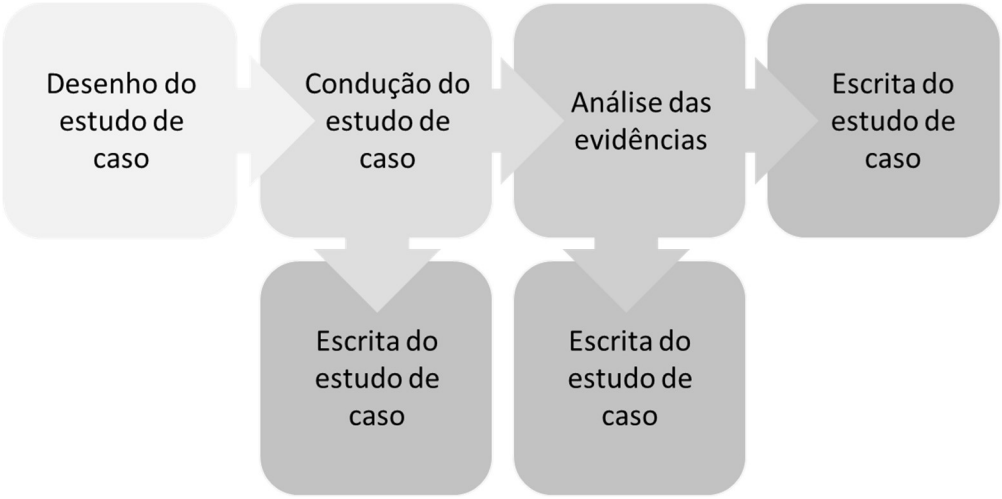


Figura 7 - Fluxo para o desenvolvimento do estudo de caso

Fonte: Elaborado pelo autor

Delimitada como um estudo de caso único, esta pesquisa buscou atender de forma satisfatória critérios metodológicos estabelecidos pela literatura, conforme pode ser observado no quadro a seguir.

Tabela 2 - Check list metodológico

PONTOS OBSERVADOS QUANTO AO OBJETO DE ESTUDO	REFERÊNCIA
O estudo busca entender um fenômeno em seu contexto real? O estudo tem por objetivo apresentar como o Privacy by Design é capaz de agregar valor às startups frente a necessidade de se adequar às exigências estabelecidas pela Lei Geral de Proteção de Dados.	YIN(2010); EISENHARDT(1989); CEPEDA e MARTIN (2005)
Qual o motivo da escolha por esta estratégia? A estratégia de se utilizar um estudo de caso com a startup Connect Point se deu pelo esforço vivenciado como CTO da startup em adequar a empresa, frente à uma exigência legal associada à uma escassez de recursos financeiros.	YIN(2010). EISENHARDT(1989); SCAPENS (1990); CESAR et al. (2010)
Existe ligação entre o fenômeno e o contexto? É importante além de entender o modelo de Privacy by Design e suas vantagens de aplicação junto às startups, entender o ambiente macro no qual está inserido o estudo de caso em questão.	YIN(2010)
Qual o tipo de questão levantada na pesquisa? A principal questão relacionada ao estudo, trata-se de como a startup Connect Point optou por se adequar às exigências da Lei e ao mesmo tempo agregar valor para seu modelo de negócio, sem a necessidade de grandes investimentos financeiros.	YIN (2010); GODOY (2006); CEPEDA e MARTIN (2005)

Qual o tipo de estudo de caso? Esse estudo busca uma investigação profunda do fenômeno contemporâneo relacionado à dificuldade das startups e pequenas empresas de se adequarem às exigências estabelecidas pela Lei Geral de Proteção de Dados, sendo classificado como um estudo descritivo.	YIN(2010); SCAPENS(1990); EISENHARDT(1989)
O caso analisado é representativo para o objetivo do trabalho? Considerando a vivência e experiência profissional, a partir dos aparentes resultados conquistados junto ao processo adotado na startup Connect Point, esse trabalho pode oferecer considerável representatividade para empresas com características semelhantes que buscam adequação à nova legislação.	GODOY(2006); YIN(2010)

PONTOS OBSERVADOS QUANTO À COLETA DE DADOS	REFERÊNCIA
Existem múltiplas fontes de evidências? De acordo com a literatura estudada, a privacidade desde a concepção de um produto ou serviço contribui de forma significativa para prevenir incidentes de privacidade e possui diferentes citações ao longo de toda evolução da era da informação. Durante o processo de observação para desenho e condução do estudo de caso, foi percebida sua aplicabilidade prática, principalmente junto à empresas em estágio inicial e *startups*.	EISENHARDT(1989); YIN(1981); GODOY (2006), CESAR et al. (2010)
Existem a triangulação entre as fontes de evidências? *(Características de confiabilidade)* As consequências negativas em caso das quebras de privacidade, embora não exploradas neste estudo de caso, é apresentada diante da literatura, e corroborando com esta premissa observa-se ao longo das entrevistas, a intensa preocupação dos usuários quanto ao tema privacidade, embora grade parte da população entrevistada não saiba como seus dados são tratados pelos controladores e operadores.	YIN(2010); MARTINS(2008); LIMA et al. (2012); CESAR et al. (2010)
Foram evidenciadas, quando necessário, medidas operacionais para as variáveis analisadas? *(Validade de construto)* Considerando as múltiplas fontes de evidência citadas na literatura bem como seus relacionamentos apresentados ao longo da evolução da era da informação, nessa pesquisa considerou-se tais premissas como medidas operacionais adequadas para os conceitos estabelecidos.	YIN(2010)
Existe explicação sobre a forma de coleta de dados como: as etapas seguidas, quando aconteceram, onde aconteceram, com quem e de que forma? *(Características de confiabilidade)* Todo processo para entendimento da percepção de usuários externos, se deu por meio da aplicação de questionários *on line*, direcionado ao público alvo e potencialmente consumidor dos serviços prestados pela *startup* utilizada para o estudo de caso. Foram aplicados em 2 momentos, sendo o primeiro em set/2021 para identificar a pretensão destes profissionais em compartilhar seus dados pessoais e profissionais e o segundo em abr/2022 para identificar o quão relevante é o tema privacidade. A primeira pesquisa já encontra-se publicada no site da *startup (https://connectpoint.com.br)* e a segunda encontra-se	YIN(2010), CESAR et al. (2010)

em fase de formatação e diagramação para publicação no mesmo ambiente.	
Existe algum relato ou indício a respeito do protocolo de pesquisa? *(Possibilidade de replicação de coleta de dados)* Como já apresentado, todo modelo de pesquisa encontra-se publicado no site da *startup (https://connectpoint.com.br)* e poderá ser replicado à qualquer momento que se fizer necessário.	YIN(2010)

PONTOS OBSERVADOS QUANTO À ANÁLISE DOS DADOS	REFERÊNCIA
Existem explicação sobre como as análises foram feitas? *(Validade interna)* A validade interna é aplicável apenas para estudos explanatórios ou causais e considerando que este trata-se de um estudo descritivo, este quesito não foi considerado.	GODOY(2006); YIN(2010)
Houve uso de teoria para embasar as análises, quando de estudo dedutivo? *(Características de validade externa)* Todas as deduções estabelecidas nesse estudo, foram embasadas no referencial teórico apresentado.	YIN(2010); OTLEY e BERRY(1994)

PONTOS OBSERVADOS QUANTO AOS RESULTADOS	REFERÊNCIA
Foram relatadas contribuições na geração do conhecimento em relação aos estudos anteriores? Esse estudo busca demonstra a aplicabilidade de metodologias desenvolvidas na década de 1990 no cenário de 2022, frente à uma Lei que representa um avanço na segurança de dados pessoais ao definir uma padronização elevada para a proteção das informações relacionadas à pessoa física.	CESAR et al. (2010); OTLEY e BERRY(1994)
O estudo alerta para pontos que ainda precisam de continuação na investigação? É importante a realização de recortes futuros com o intuito de validação das premissas teóricas nas quais esse estudo foi embasado, identificando não somente o nível de confiança apresentado pelos titulares dos dados como também o quanto o modelo contribuiu para a confiança de investidores e parceiros.	CESAR et al. (2010)

Fonte: Elaborado pelo autor

Considerando as características do Mestrado Profissional, com a metodologia aplicada durante o trabalho, torna-se possível atender à uma necessidade real de mercado da startup Connect Point, com a utilização de estudos e pesquisas fundamentadas em conceitos já consolidados pela academia. Diante do desafio já proposto pela linha de pesquisa, “Sistemas de inovação e de desenvolvimento:

aspectos jurídicos, econômicos e sociais”, o estudo de caso da Connect Point permite uma visão geral de todos os aspectos envolvidos diante de uma necessidade de mercado, capaz de proporcionar não somente um reposicionamento da empresa perante à clientes e futuros investidores, mas também ao atendimento de uma nova legislação.

4. A CONNECT POINT

Muitas empresas certamente já tentaram participar de um procedimento licitatório e não conseguiram, por não atingirem algum requisito de qualificação técnica ou econômica. Considerando o requisito de qualificação técnica, se as empresas tivessem a oportunidade de se unir à profissionais com as qualificações técnicas específicas para completar os requisitos exigidos, sua participação talvez seria mais favorável.

Com o objetivo de conectar experiências profissionais de forma simples, rápida e focada nas demandas dos mercados de arquitetura e engenharia, a Connect Point possui uma plataforma que também auxilia as empresas para o recebimento de avisos sobre licitações relacionadas com as suas áreas de atuação.

4.2. Reconhecendo o perfil do público alvo

Em 2021, foi realizado por meio das redes de relacionamento da Connect Point, uma pesquisa junto a profissionais que atuam nos mercados de arquitetura e de engenharia para conhecermos um pouco melhor sobre o perfil desta população a fim estabelecer as ações para o fortalecimento da atuação da Connect Point.

Para esta pesquisa, foi elaborado um formulário via Google Forms[44] e enviado via WhatsApp[45] e e-mail para um público de 534 profissionais, sendo 527 no Brasil, 5 nos Estados Unidos e 2 em Portugal. Desse total, obtivemos 261 respostas e esse resultado só foi possível devido ao compartilhamento da pesquisa por muitos que a receberam, junto às suas próprias redes de relacionamento.

Nesta primeira pesquisa, obtivemos a identificação da formação acadêmica, tempo de formação, vínculo profissional, atuação profissional, experiências,

[44] Google Forms é um aplicativo de gerenciamento de pesquisas lançado pelo Google. Os usuários podem usar o Google Forms para pesquisar e coletar informações sobre outras pessoas e também podem ser usados para questionários e formulários de registro.

[45] WhatsApp é um aplicativo multiplataforma de mensagens instantâneas e chamadas de voz para smartphones. Além de mensagens de texto, os usuários podem enviar imagens, vídeos e documentos em PDF, além de fazer ligações grátis por meio de uma conexão com a internet.

comprovações de experiência e outras, que foram responsáveis por viabilizar a formação do que foi conceituado como CIC – Conselho de Inovação da Connect.

4.2.1. Formação acadêmica

Do público entrevistado, 61% dos respondentes são considerados como foco da pesquisa, uma vez que são formados em engenharia civil ou arquitetura, sendo 33% formado em Engenharia Civil e 28% formado em Arquitetura e Urbanismo. As demais formações identificadas foram Engenharia Elétrica (9%); Engenharia Sanitária e/ou Ambiental (7%); Ciências Biológicas e Geologia (3% cada); Engenharia de Produção, Geografia, Engenharia Química, Engenharia Mecânica e Design de Interiores (2% cada); e os 7% restantes, outras formações, conforme distribuição absoluta representada no gráfico 1 a seguir:

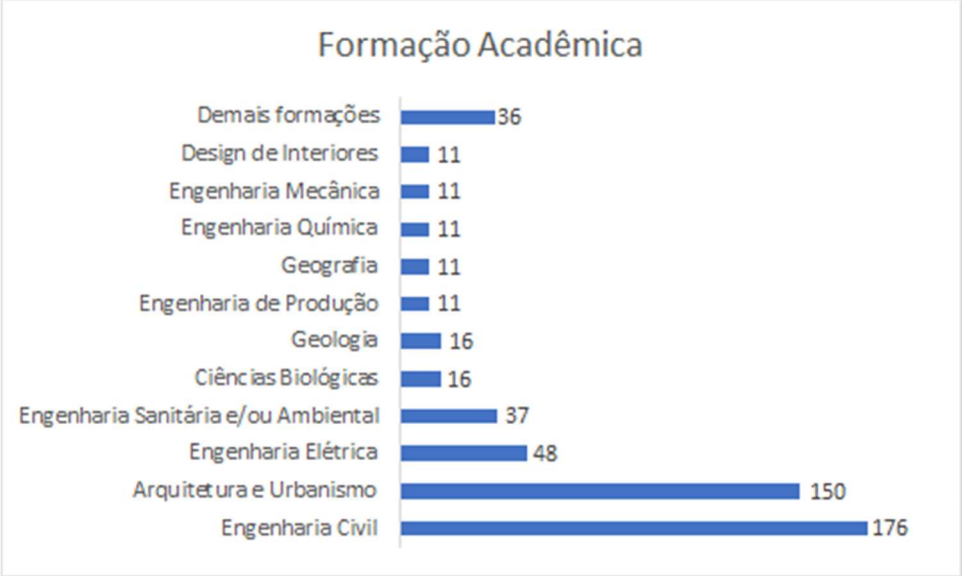


Gráfico 1 - Formação Acadêmica
Fonte: *Google forms elaborado pelo autor*

4.2.2. Tempo de formação

Do público entrevistado, 67% têm acima de 10 anos de formado; 12% entre 5 e 10 anos de formado; 10% entre 2 e 5 anos de formado; 8% até 2 anos de formado; e 3% ainda não se formaram, conforme distribuição absoluta representada no gráfico 2 a seguir:

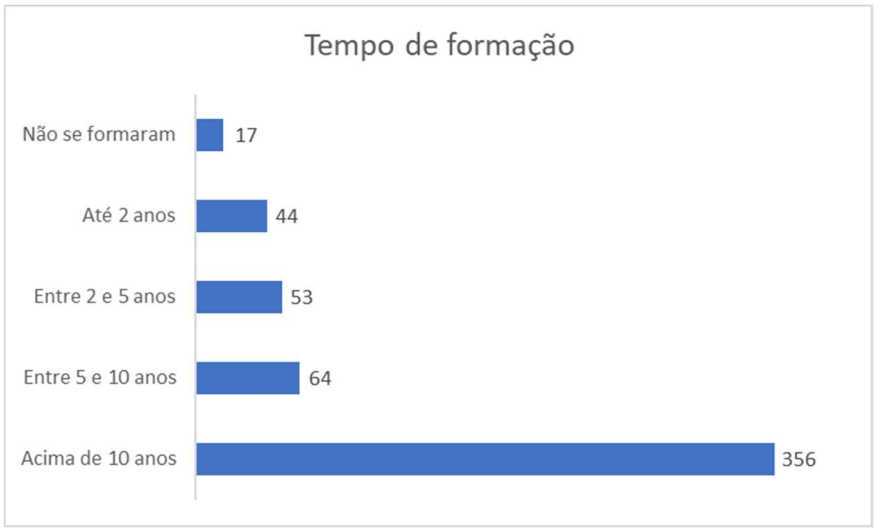


Gráfico 2 - Tempo de formação
Fonte: *Google forms elaborado pelo autor*

4.2.3. Vínculo profissional

Do público entrevistado, 31% são empregados(as); 27% profissionais liberais/autônomos(as); 25% empresários(as); 7% funcionários públicos; 7% não trabalham; 3% são estagiários, conforme distribuição absoluta representada no gráfico 3 a seguir:

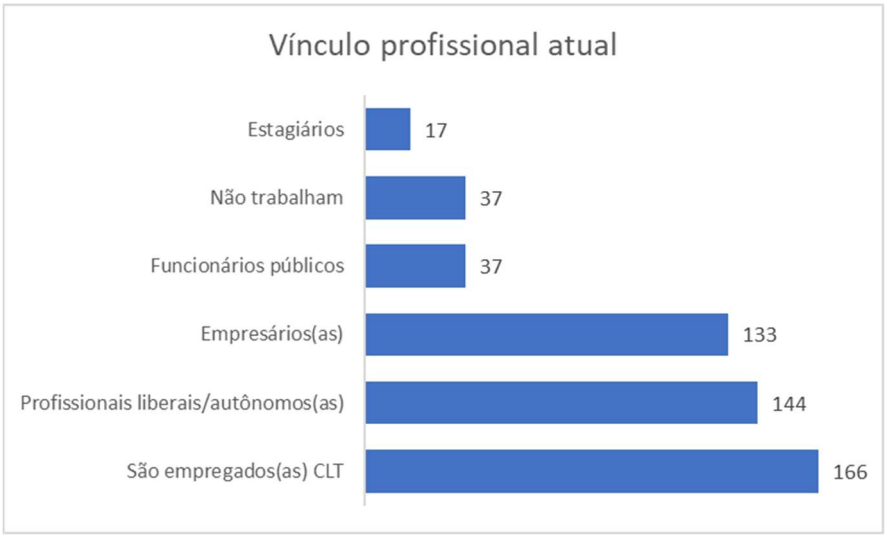


Gráfico 3 - Vínculo profissional atual
Fonte: *Google forms elaborado pelo autor*

4.2.4. Área de atuação

Perguntados se trabalham na sua área de formação, do total entrevistado, 82% responderam que sim; 14% que não e 4% responderam estarem desempregados(as), conforme distribuição absoluta representada no gráfico 4 a seguir:

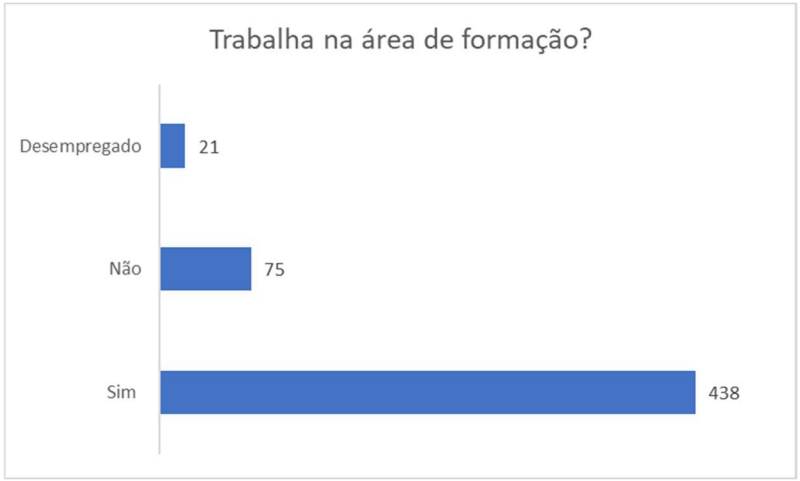


Gráfico 4 - Trabalha na área de formação
Fonte: *Google forms elaborado pelo autor*

4.2.5. Experiência profissional

Dos 534 entrevistados, a grande maioria – ou seja, 59% – prestam serviços para o setor privado; 24% para o setor público; 16% trabalham para o serviço público e 1% não possui experiência na sua área de formação, conforme distribuição absoluta representada no gráfico 5 a seguir:

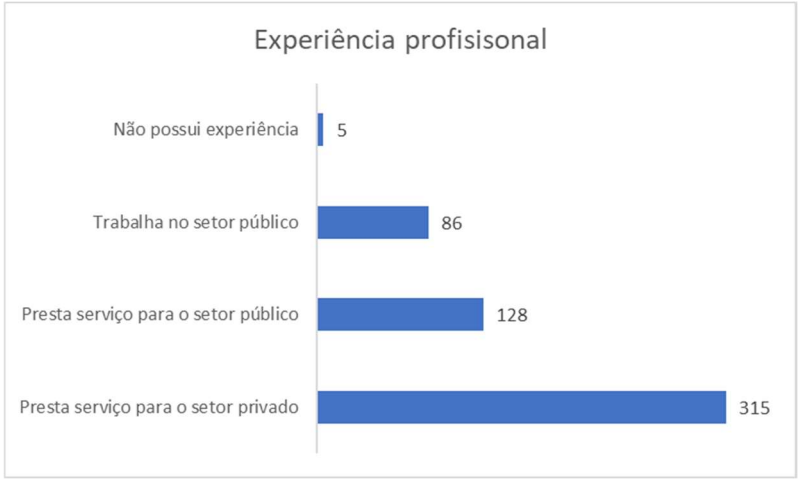


Gráfico 5 - Experiência profissional
Fonte: *Google forms elaborado pelo autor*

4.2.6. Comprovação de experiência

Considerando que um ponto relevante para a participação de licitações é a comprovação da experiência, 35% dos entrevistados informaram que podem comprovar a experiência por meio de ART, RRT ou similar; 25% por meio de atestados e/ou declarações; 16% não possuem comprovações; 15% comprovam por meio de Certidão de Acervo Técnico (CAT); 4% por meio de carteira de trabalho e os 5 % restantes por meio de contratos de prestação de serviços; currículo, portfolio e outras comprovações, conforme distribuição absoluta representada no gráfico 6 a seguir:

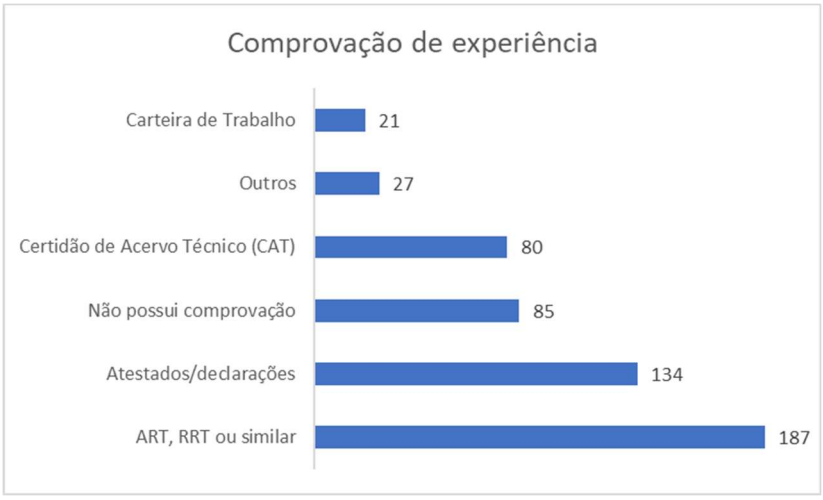


Gráfico 6 - Comprovação de experiência
Fonte: *Google forms elaborado pelo autor*

4.2.7. Abertura para ofertas de trabalho

Com o objetivo de identificar quais profissionais estariam abertos para receber ofertas de trabalho/emprego, 75% responderam que sim e 25% que não, conforme distribuição absoluta representada no gráfico 7 a seguir:

Gráfico 7 - Aberto para ofertas de trabalho/emprego
Fonte: *Google forms elaborado pelo autor*

4.2.8. Meios de busca por novas oportunidades

Ao serem questionados quanto aos meios de busca por novas oportunidades de trabalho, 24% dos entrevistados responderam ser por meio de contatos pessoais; 23% pelo LinkedIn; 14% por sites de vagas; 13% por sites de empresas; 11% por grupos de WhatsApp; 7% por Instagram; 5% por headhunter; 2% por Facebook; 1% não procura e o restante em outros meios, conforme distribuição absoluta representada no gráfico 8 a seguir:

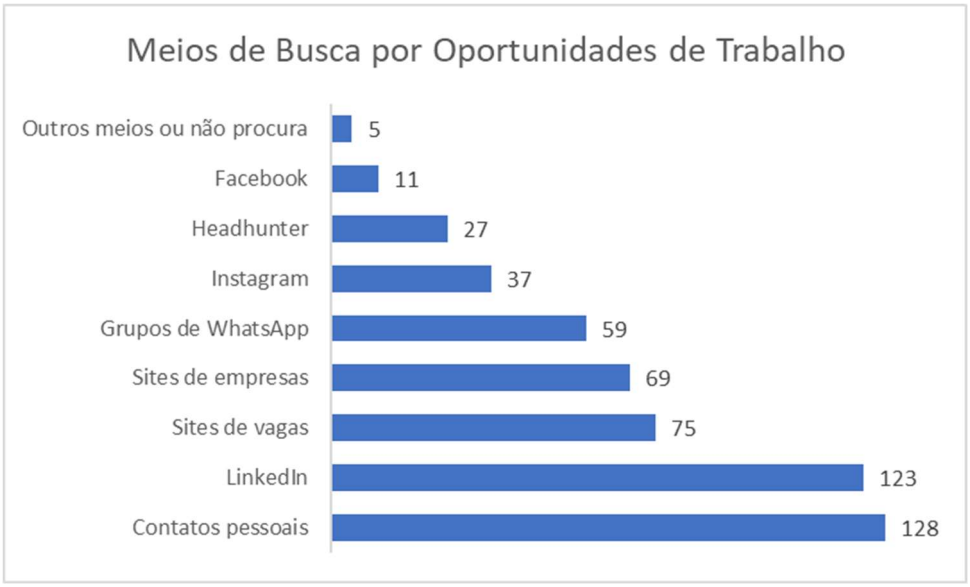


Gráfico 8 - Meios de busca por oportunidades de trabalho
Fonte: *Google forms elaborado pelo autor*

4.2.9. Atualizações sobre o Mercado de Trabalho

Com relação às atualizações sobre o mercado de trabalho, 20% dos entrevistados informaram ser por meio da Internet; 17% por meio de cursos; 15% com eventos da área; 13% pelo LinkedIn; 7% pelo Instagram; 7% por sites de empresas; 5% por Newsletters institucionais; 1% pelo Facebook e o restante por outros meios, conforme distribuição absoluta representada no gráfico 9 a seguir:

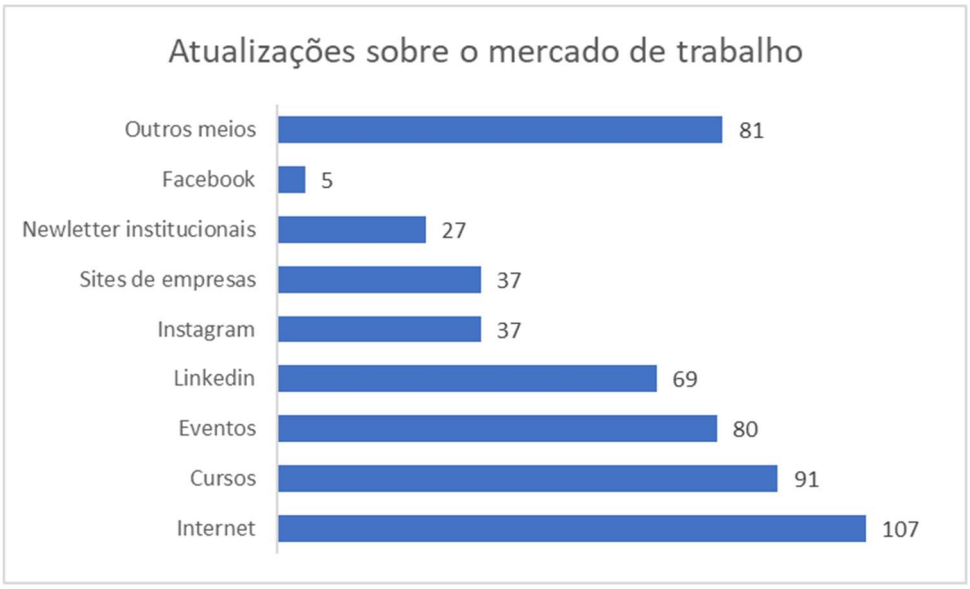


Gráfico 9 - Atualizações sobre o mercado de trabalho
Fonte: *Google forms elaborado pelo autor*

4.2.10. Foco na entrega

Com o objetivo de identificar a aceitação de uma plataforma com as características da Connect Point que é a de relacionar a oferta com a demanda de uma mão de obra especializada, realizamos 2 perguntas finais, de forma direta e objetiva, sendo a primeira para saber do entrevistado se ele se cadastraria em um canal especializado em oportunidades profissionais de sua área de formação e/ou atuação e o que ele gostaria que tivesse de conteúdo nesse canal. As respostas representadas de forma absoluta, poderão ser avaliadas nos gráficos 10 e 11 a seguir:

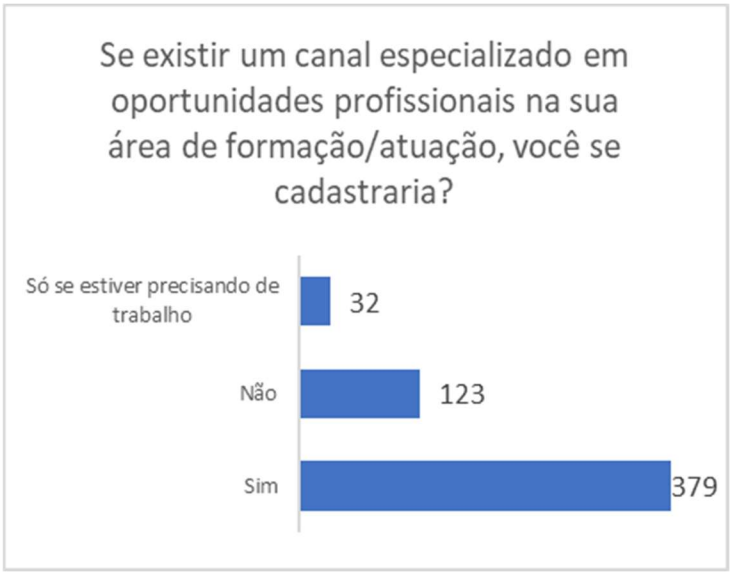


Gráfico 10 – Interesse por uma plataforma
Fonte: *Google forms elaborado pelo autor*

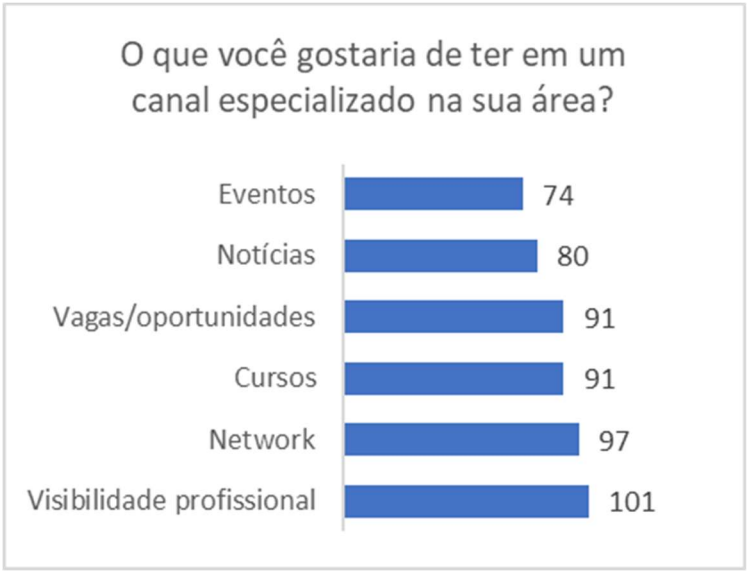


Gráfico 11 - Expectativa de conteúdo
Fonte: *Google forms elaborado pelo autor*

4.3. Primeiras impressões

Considerando que a maior parte dos entrevistados – 61%, possui formação na principal área em que a Connect Point busca maior atuação, o resultado apresentado demonstrou que a população entrevistada possui larga experiência atuação correspondente à área de formação, podendo comprovar toda a experiência por diferentes meios, o que pode ser fator decisivo em processos licitatórios.

Nesta primeira avaliação, observou-se que os entrevistados buscam não somente novas oportunidades, mas também capacitação e aperfeiçoamento por meio das redes de relacionamento e plataformas digitais favorecendo o modelo de negócio proposto pela Connect Point.

Ao final, a pergunta direta objetivando identificar a aceitação por uma plataforma responsável por conectar competências e proporcionar visibilidade profissional, teve excelente aceitação pelos respondentes, direcionado nosso desenvolvimento para as necessidades apresentadas pelo público entrevistado.

4.4. A preocupação com a privacidade

Diante do novo desafio apresentado pela Lei Geral de Privacidade de Dados associado ao desafio da construção de uma plataforma que tem seu principal objetivo o tratamento de competências pessoais, a Connect Point associou a experiência profissional de sua liderança bem como as referências e boas práticas oferecidas pela literatura para proporcionar privacidade e segurança à seus clientes e parceiros, sendo também compreendido, que dificilmente uma startup receberá um bom aporte de investimento se possuir um grande passivo, especialmente no que tange a segurança de dados pessoais.

A partir daí, foram iniciadas pesquisas com o intuito de identificar metodologias simples e eficazes, capazes de proporcionar privacidade principalmente ao se considerar uma empresa recém criada, sempre ressaltando que considerando a severidade das penas estabelecidas pela LGPD que vão desde elevadas multas até a exclusão definitiva de bancos de dados, qualquer fator a favor das *startups* pode ser fator decisivo para o sucesso.

Ainda relacionado às penalidades previstas pela LGPD, é importante considerar que na dosimetria da pena prevista pela lei, a Autoridade Nacional de Proteção de Dados - ANPD[46], ao apurar uma infração, poderá ter como um dos critérios para redução de penalidades a avaliação se o negócio já foi desenhado prezando pelo respeito à privacidade e aos direitos fundamentais dos titulares.

Os estudos e pesquisa relacionados à privacidade, nos deixam a impressão de que o ponto principal para este sucesso é o que consideramos ser uma “cultura de privacidade” e para introduzir esta cultura, de acordo com toda literatura pesquisada, o *privacy by design* poderia ser o grande diferencial.

Todas os passos, ideias, produtos, funcionalidades devem ter como foco a privacidade do usuário e a proteção de suas informações pessoais, ou seja, a proteção de dados é colocada no centro do desenvolvimento de todo projeto, sendo esse valor incorporado pela empresa, diretores e colaboradores. É importante que ninguém pense ou desenvolva nada que não tenha a privacidade ou a proteção de dados pessoais como plano de fundo.

De fato, não é fácil trazer esse conceito para o dia a dia, principalmente quando se tem pouca ou nenhuma prática na proteção de dados pessoais de clientes ou usuários.

4.5. A pesquisa sobre privacidade

Uma vez identificado o perfil do público alvo e diante dos desafios relacionados à privacidade e proteção de dados, em 2022, foi aplicada uma nova pesquisa para os participantes da pesquisa de 2021, porém desta vez, o objetivo foi identificar a importância da privacidade na visão destes usuários.

Embora a pesquisa anterior tivesse retornado 261 respostas, esta nova pesquisa retornou 213 respostas, sendo que mesmo não tendo campo para que o

[46] A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão da administração pública direta federal do Brasil que faz parte da Presidência da República e possui atribuições relacionadas a proteção de dados pessoais e da privacidade e, sobretudo, deve realizar a fiscalização do cumprimento da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD).

usuário realizasse uma descrição livre, muitos encaminharam comentários extra formulário, conforme representado na figura 8, com relatos do tipo:

"Assunto de extrema relevância, parabéns pela preocupação."

"Já fui vítima de fraude e tenho receio de passar meus dados."

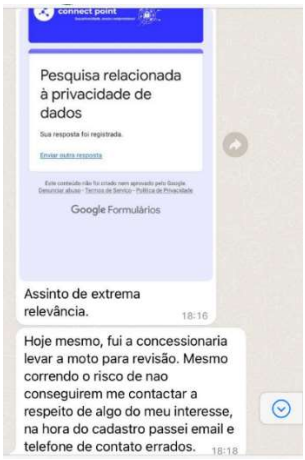


Figura 8 - Feedback recebido via aplicativo WhatsApp

4.5.1. Relacionamento com a empresa

Do público entrevistado, 93% dos respondentes não possuem nenhum relacionamento com a Connect Point, 6% já são profissionais com suas experiências profissionais compartilhadas com a Connect Point e apenas 1% trata-se de empresas que buscam esses profissionais junto à plataforma Connect Point. A distribuição absoluta destes respondentes pode ser observada no gráfico 12 a seguir:

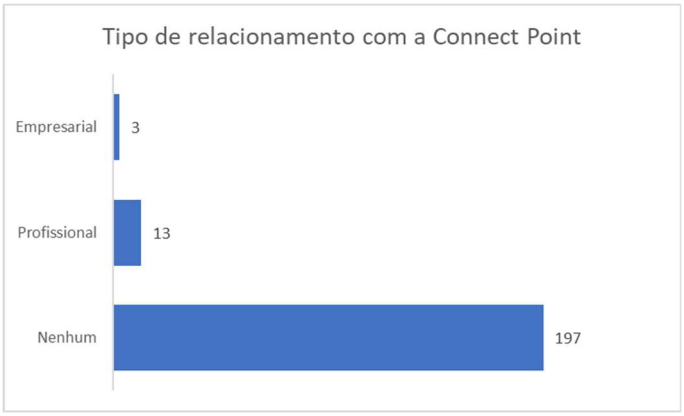


Gráfico 12 - Tipo de relacionamento com a Connect Point
Fonte: *Google forms elaborado pelo autor*

4.5.2. Segurança em compartilhar os dados pessoais com a Connect Point

Dos 16 respondentes que possuem algum relacionamento com a Connect Point, mesmo sem uma cultura de privacidade totalmente estabelecida na empresa, o resultado apresentado pode ser considerado satisfatório, uma vez que ao menos a sensação de segurança está sendo retransmitida aos usuários. 50% destes respondentes se sentem completamente seguros em compartilhar os dados com a Connect Point e os outros 50% ainda se sentem parcialmente seguros. A distribuição absoluta deste resultado pode ser observada no gráfico 13 a seguir:

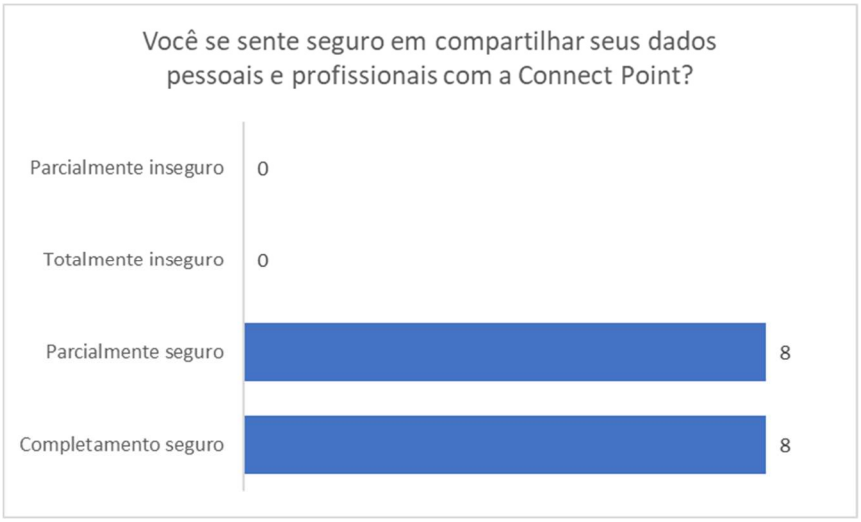


Gráfico 13 – Segurança em compartilhar dados pessoais com a Connect Point
Fonte: *Google forms elaborado pelo autor*

4.5.3. Prática de compartilhamento de dados

A solicitação de dados pessoais é hoje bastante intensa não somente nas plataformas digitais como nos meios físicos. Esta abordagem se tornou atualmente tão comum quando buscamos algum serviço ou produto que nos sentimos constrangidos em perguntar o porquê.

Com base nesta realidade, foi questionado aos entrevistados se eles possuem o costume de compartilhar seus dados pessoais com outras empresas e o resultado de certa forma surpreendeu, uma vez que mais da metade dos respondentes informaram que raramente costumam compartilhar seus dados pessoais. A distribuição absoluta deste resultado pode ser observada no gráfico 14 a seguir:

Gráfico 14 - Costume em compartilhar dados pessoais
Fonte: *Google forms elaborado pelo autor*

4.5.4. Clareza no tratamento de dados

Todos os dias, as pessoas realizam pesquisas e compras via internet, instalam e utilizam diferentes aplicativos, realizam o preenchimento de cadastros de serviços em diversos meios e tudo isso gerando e compartilhando centenas de milhares de dados pessoais. Este intenso tratamento de dados pessoais em sua grande maioria, não apresenta ao usuário a real necessidade da coleta nem mesmo o que são feitos com estes dados.

É importante ressaltar que a LGPD fortalece o conceito de que o “dono” do dado é o titular e não quem os detêm por algum motivo. De forma geral, considerando os 10 princípios de tratamento de dados pessoais estabelecidos pela LGPD, a grande maioria envolve clareza e transparência.

Diante deste cenário, foi questionado aos entrevistados se existe clareza de como os dados que são disponibilizados às empresas são tratados. Como já era esperado, a grande maioria, 91%, relatou não ter clareza de como seus dados são tratados às empresas. A distribuição absoluta deste resultado pode ser observada no gráfico 15 a seguir:

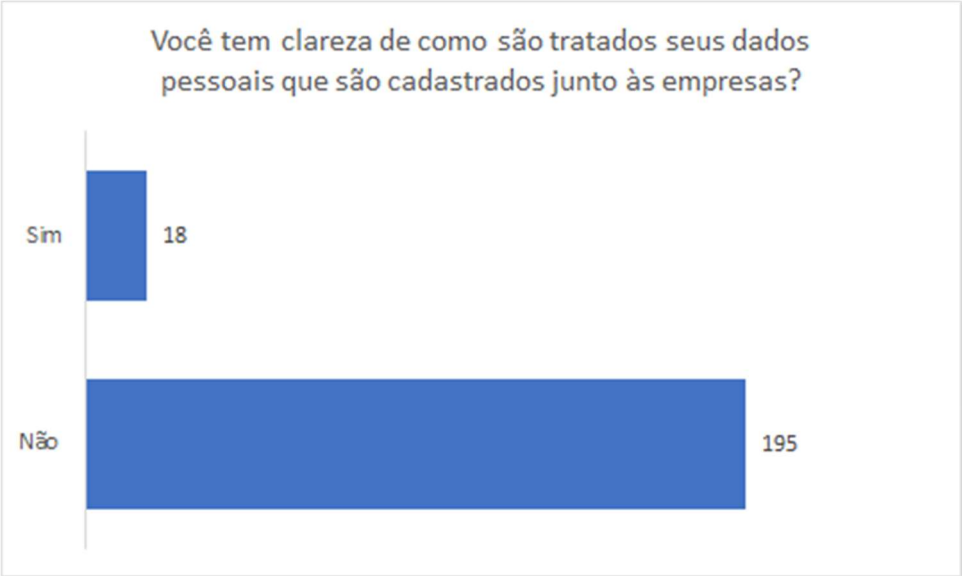


Gráfico 15 - Clareza no tratamento de dados
Fonte: *Google forms elaborado pelo autor*

4.5.5. A importância da gestão de dados pessoais

Toda empresa que utiliza dados pessoais precisa aprender a usar os elementos que resultam da privacidade como um aliado do negócio. A privacidade de dados também pode representar um diferencial competitivo, considerando que a cada dia que passa as pessoas buscam relações com organizações éticas e responsáveis.

Se a natureza da operação da empresa, exige o uso de dados pessoais é importante entender que a privacidade e a segurança de dados é responsabilidade de todos os departamentos da organização e não apenas das áreas de tecnologia e segurança da informação.

A tendência é que empresas genuinamente interessadas em se tornarem organizações evoluídas que entendem a importância da privacidade de dados pessoais sejam vistas pelos clientes como as melhores companhias para se estabelecer relacionamentos.

Todo este arcabouço teórico foi percebido com clareza diante do questionamento aos entrevistados, quando os mesmos se posicionaram em relação à importância de uma boa gestão dos dados pessoais junto às empresas nas quais são compartilhados os dados pessoais. Mais de 80% dos respondentes, consideraram

que é importante ou muito importante uma boa gestão de dados pessoais, e a distribuição absoluta deste resultado pode ser observada no gráfico a seguir:

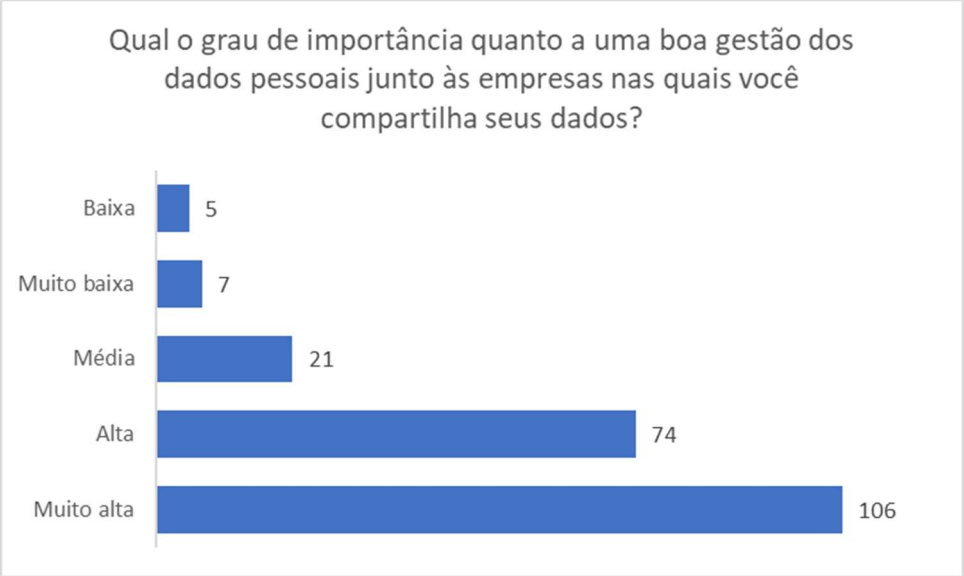


Gráfico 16 - Importância da gestão dos dados
Fonte: *Google forms elaborado pelo autor*

4.6. A privacidade na visão do usuário

Com o resultado desta segunda pesquisa, observou-se que a preocupação com a privacidade dos dados é realmente um fator de destaque diante da população entrevistada. 84% dos respondentes, consideram que uma boa gestão dos dados possui um grau de importância alta e muito alta, porém mesmo considerando que quase a metade deste público compartilha seus dados com certa frequência, 92% não tem clareza de como seus dados são tratados junto às empresas.

Corroborando com o resultado apresentado nesta pesquisa, foi identificado uma publicação da IBM de dezembro de 2019, que apontou que 96% dos brasileiros acreditam que as empresas não protegem seus dados pessoais. Nesta pesquisa, realizada em 11 países, incluindo o Brasil, com cerca de 11 mil pessoas, apontou que os consumidores em todo o mundo estão demandando às organizações mais transparência e controle sobre seus dados.

De acordo com The Harris Polls[47], empresa que realizou a pesquisa encomendada pela IBM, os resultados indicam que as pessoas estão insatisfeitas com a maneira com que muitas empresas lidam com suas informações: 96% dos consumidores pesquisados no Brasil concordam que as organizações devem fazer mais para protegê-los. Nos demais países onde a pesquisa foi conduzida, mais da metade dos entrevistados concorda com essa afirmação. Além disso, segundo o levantamento, 6 em cada 10 brasileiros relataram que sofreram com vazamento de dados ou conhecem alguém que tenha passado pela situação.

Quando se trata de privacidade, não há uma preocupação apenas com a proteção, mas também com o controle dos dados. No Brasil, 5 em cada 10 consumidores sabem que suas informações são sempre, ou na maioria das vezes, compartilhadas. De fato, 81% dos brasileiros afirmaram ter perdido o controle de como suas informações pessoais são usadas pelas empresas.

Segundo João Rocha, líder de segurança da informação da IBM Brasil, as organizações precisam repensar sua abordagem em relação à responsabilidade de dados, especialmente com a chegada da Lei Geral de Proteção de Dados.

> *"Temos à nossa disposição novas tecnologias que, por meio dos dados, podem impulsionar a inovação, como Inteligência Artificial, Cloud e Blockchain. No entanto, empresas que coletam, armazenam, gerenciam ou processam dados têm a obrigação de tratá-los com responsabilidade e a LGPD assegurará isso. Por isso, é importante que as organizações comecem a se preparar o quanto antes e concentrem seus esforços na segurança e privacidade."*
>
> *João Rocha, head de cibersegurança da IBM Brasil.*

Rocha também afirma que proteger as informações dos clientes, pode refletir uma vantagem competitiva para as empresas, uma vez que os clientes valorizam empresas que são seguras em relação ao tratamento de seus dados.

[47] The Harris Polls, é uma empresa americana de pesquisa e análise de mercado que acompanha o sentimento, comportamentos e motivações dos adultos americanos desde 1963.

Todo este cenário identificado, contribui para o fortalecimento estratégico da Connect Point em investir na cultura da privacidade de dados da empresa, oferecendo não somente a privacidade de dados aos usuários como também a confiança e transparência durante todo o tratamento de dados realizado.

4.7. O processo de implantação do *Privacy by Design*

Uma vez identificada algumas das dores dos clientes relacionadas à privacidade de dados, bem como a importância de apresentar ao mercado uma empresa aderente à legislação no que tange ao tema, a Connect Point estrutura seu reposicionamento ao mercado, com foco no investimento em privacidade e proteção da dados pessoais conforme necessidade identificada.

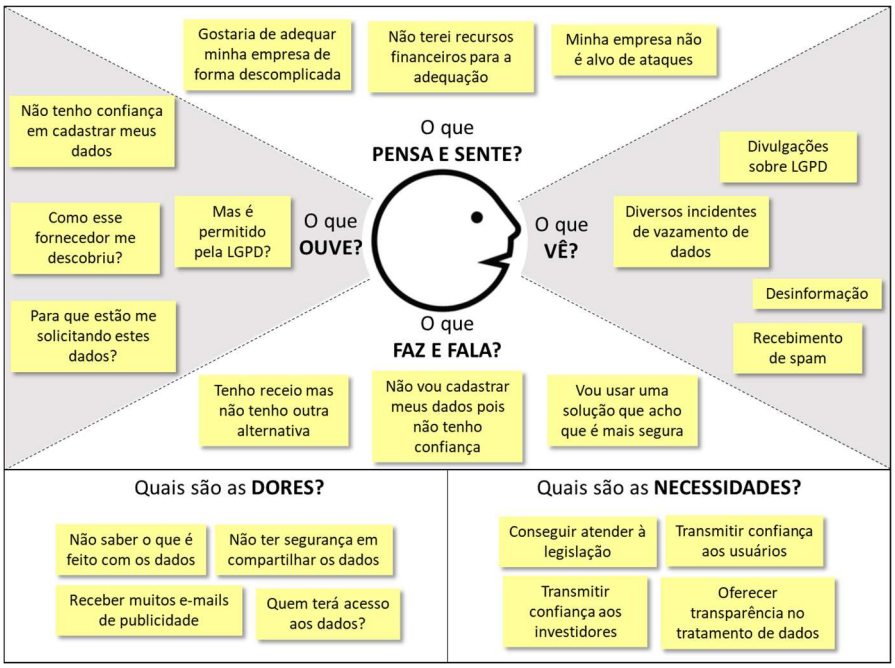


Figura 9 - Mapa de empatia
Fonte: *Elaborado pelo autor*

Considerando que garantir e respeitar os interesses dos usuários com relação ao tratamento de seus dados é uma das maiores preocupações previstas pelo *Privacy by Design*, a primeira ação realizada foi a capacitação e alinhamento de toda equipe quanto ao tema privacidade.

Em um segundo momento, foi realizado o levantamento de todos os requisitos internos e externos relacionados à segurança da informação, traçando um mapa de

riscos, considerando o impacto x probabilidade de vazamento de dados, bem como planos de ação capazes de mitigar os riscos.

Na etapa seguinte, a preocupação foi de entender e mapear todo o ambiente informacional, remodelando bancos de dados, servidores de testes e aplicações, identificação de casos de uso além da avaliação quanto aos princípios de uso e bases legais.

Visando garantir uma boa condição de segurança, foram implementadas também como parte do processo do *Privacy by Design*, a estruturação de testes de segurança por meio de parcerias com empresas especializadas e os resultados dos testes serviram para aperfeiçoamento de todo ambiente.

Como a LGPD é orientada a processos podemos utilizar ferramentas já estabelecidas, como o PDCA[48], para garantir a continuidade do *Privacy by Design* uma vez que sempre será necessário ajustar, reavaliar e refinar o plano de adequação.

Com o objetivo facilitar o entendimento da metodologia aplicada junto à Connect Point para a implementação do *Privacy by Design*, o processo descrito pode ser resumido em diagnosticar, operacionalizar e promover meios de sustentação do modelo aplicado, conforme ilustração a seguir:

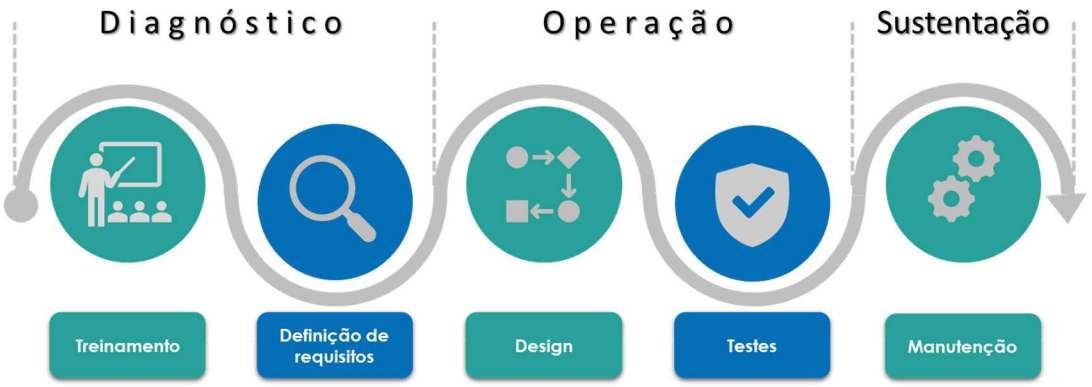


Figura 10 - Processo para implementar o Privacy by Design
Fonte: *Elaborado pelo autor*

[48] PDCA é um método iterativo de gestão de quatro passos, utilizado para o controle e melhoria contínua de processos e produtos. É também conhecido como o círculo/ciclo/roda de Deming, ciclo de Shewhart, círculo/ciclo de controle, ou PDSA

4.7.1. Treinamento

Assim como a grande maioria das *startups*, a Connect Point possui uma equipe pequena, composta por apenas 04 (quatro) profissionais, sendo que 02 (dois) já estão completamente envolvidos no contexto da LGPD e privacidade de dados facilitando o nivelamento do conteúdo e fortalecendo para o início da implantação da cultura de privacidade.

Como primeira parte do treinamento, foi apresentado e debatido entre o grupo, situações simples do dia a dia, no qual a privacidade não é percebida fator de relevância pelos usuários. Neste momento também foi realizado o estudo e caracterização de casos já identificados diante do ambiente profissional, apontando falhas e planos de mitigação, sem ainda o fortalecimento da base conceitual de segurança e privacidade de dados.

Na segunda etapa do treinamento, foram apresentados aos colaboradores, os conceitos básicos da legislação, bem como os princípios de tratamento de dados e as bases legais previstas. É bastante importante neste momento, que o repasse de informação seja algo realizado por meio de uma linguagem natural, sem o uso desnecessário e excessivo do jargão jurídico e de termos técnicos do direito.

Visando garantir o nivelamento de toda equipe e também uma constante atualização do contexto de privacidade e proteção de dados, foi estabelecido entre a equipe, que campanhas de conscientização deverão ser continuamente desenvolvidas e todo novo colaborador da *startup* deverá passar por um treinamento básico introdutório – TBI, com o objetivo de nivelar os conceitos relacionados às práticas de privacidade.

4.7.2. Definição dos requisitos

Levando em consideração as melhoras práticas de implantação do *Privacy by Design*, foi discutido entre o grupo a necessidade da implantação de um comitê de privacidade. Considerando o tamanho da equipe, ficou estabelecido embora um comitê formal ainda não fosse necessário, o advogado de direito digital da *startup*, que possui amplo conhecimento em relação às regras estabelecidas pela LGPD, seria o

responsável por orientar e instruir toda equipe sobre o tema privacidade, além de promover um programa de governança em privacidade identificando as necessidades gerais e específicas, assumindo também as atribuições de DPO (*Data Protection Officer*) ou Encarregado de Dados.

Este programa de governança em privacidade, deverá envolver a elaboração de políticas e procedimentos que garantam a correta adequação a LGPD e demais políticas de proteção de dados pessoais nas quais a Connect Point necessite adequação. Neste roteiro, serão desenvolvidos os seguintes instrumentos normativos:

i. Política de Privacidade de uso interno;
ii. Aviso de Privacidade para usuários externos;
iii. Relatório de impacto de proteção de dados;
iv. Plano de respostas à incidentes.

Uma vez elaborados, estes instrumentos normativos de privacidade deverão ser submetidos para a avaliação dos demais fundadores da Connect Point e publicados como documentos oficiais de privacidade e proteção de dados pessoais.

4.7.2.1. Política de Privacidade

A política de privacidade é um documento interno dirigido a funcionários e eventuais prestadores de serviço. Este documento será o responsável por informar como dados pessoais serão tratados, armazenados e transmitidos para atender às necessidades organizacionais e as legislações aplicáveis, definindo todos os aspectos relativos à proteção de dados, incluindo como o aviso de privacidade será formado.

A política de privacidade deverá ser considerada por toda a *startup*, desde seus fundadores, administradores, investidores e demais membros da equipe de que alguma forma esteja envolvida na operacionalização das atividades. Esta política de privacidade, ou simplesmente PP, deverá ser clara, compreensível, acessível e abrangente à toda atividade da *Connect Point*. Os principais componentes desta PP são:

a. **Objetivo:** apresenta o motivo da elaboração da política e as principais metas a serem atingidas;
b. **Escopo:** apresenta os recursos nos quais a política visa proteção, seja estes recursos físicos, processos ou tecnologias;
c. **Responsabilidade:** descreve de forma detalhada o papel de cada profissional envolvido em processos relacionados à proteção de dados, incluindo membros da Connect Point e terceiros;
d. **Conformidade:** estrutura para garantir a adequação às normas aplicáveis, incluindo políticas e procedimentos administrativos tais como política de controle de acesso e até mesmo regime de sanções disciplinares por descumprimento à política de privacidade.

4.7.2.2. Aviso de Privacidade

Embora em muitos portais disponibilizados nos meios eletrônicos tratem os avisos de privacidade como “políticas de privacidade” o aviso de privacidade em sua essência, trata-se de uma comunicação externa para titulares de dados que não componham a instituição. Desta forma, um aviso de privacidade descreve de forma clara e objetiva como os dados são coletados, usados, compartilhados e até mesmo armazenados e divulgados com base na política de privacidade estabelecida.

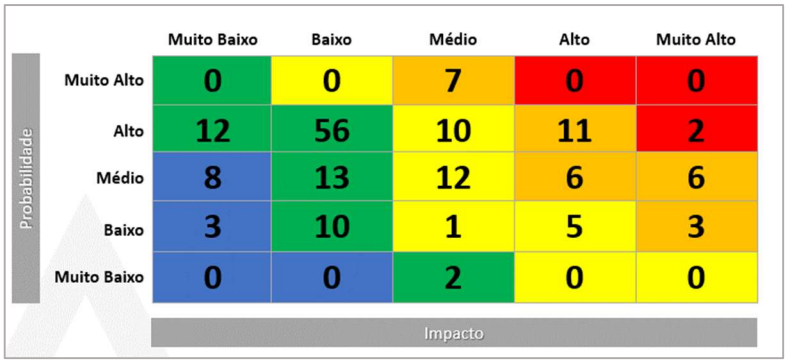
4.7.2.3. Relatório de impacto de proteção de dados

O Relatório de Impacto de Proteção de Dados - RIPD, é uma análise dos riscos à proteção de dados associados ao tratamento de dados pessoais em relação a um determinado projeto, produto ou serviço. O RIPD também deve sugerir ou fornecer ações corretivas ou mitigações necessárias para evitar ou mitigar esses riscos.

A Connect Point, realiza um estudo detalhado de cada dado tratado, elaborando uma matriz 5x5, considerando a probabilidade x impacto no caso de vazamento de dados.

No eixo da probabilidade, são avaliadas as probabilidades de vazamento de dados, considerando o perfil de segurança identificada junto aos departamentos e este perfil recebe uma pontuação de acordo com cada cenário. No eixo impacto, são

consideradas as avaliações de cada dado tratado, avaliando o impacto de acordo com a classificação de dados sensíveis ou não, descritas na LGPD – Lei Geral de Proteção de Dados. Após o cruzamento dos valores de avaliações identificadas, são apresentados os totais de dados com cada uma das classificações obtidas.



Probabilidade	Muito Baixo	Baixo	Médio	Alto	Muito Alto
Muito Alto	0	0	7	0	0
Alto	12	56	10	11	2
Médio	8	13	12	6	6
Baixo	3	10	1	5	3
Muito Baixo	0	0	2	0	0

Figura 11 - Matriz de riscos
Fonte: *Elaborado pelo autor*

Embora até o momento não haja a determinação da ANPD – Autoridade Nacional de Proteção de Dados as hipóteses em que tal relatório seja necessário, considerando as boas práticas identificadas diante de outras Leis de Privacidade, assim como a *Information Commissioner's Office* – ICO, do Reino Unido e a francesa *Commission Nationale de l'Informatique et des Libertés* – CNIL, a Connect Point julga importante estabelecer mais este mecanismo de controle.

A ABNT NBR ISO/IEC 29134, normativo que trata diretamente de tecnologia da informação e privacidade, em vigor e publicada em 26 de novembro de 2020, também é outro importante instrumento para condução e elaboração do RIPD elaborado. De forma resumida, a ISO 29134, estabelece 4 etapas fundamentais para a elaboração de uma RIPD:

a. **Análise preliminar**: conduzir uma análise preliminar de riscos, para determinar se o RIPD é necessário. Se for concluído por existência de atividades de alto risco, a elaboração do RIPD deve ser conduzida;
b. **Preparação do RIPD**: coleta de informações sobre as operações de tratamento. O inventário de dados pessoais e o *gap analysis* são dois procedimentos importantes nessa etapa preparatória;
c. **Elaboração do RIPD:** identificar o escopo do tratamento, determinar os requisitos de proteção de dados relevantes (princípios, bases legais,

direitos dos titulares, transferências internacionais, etc.), acessar o risco (identificação, análise e avaliação do risco) e elaborar o plano tratamento do risco (medidas técnicas e administrativas *security by design* e *privacy by design*).

d. **Monitoramento do RIPD**: preparar e publicar o relatório, implementar o plano de tratamento de risco, revisar o relatório.

4.7.2.4. Plano de resposta a incidentes

No mundo real, o risco zero não existe. Isso porque, em tudo que fazemos, há sim a possibilidade de ocorrer um imprevisto, um erro, e tudo muda em uma simples tarefa rotineira. De acordo com Antônio Mendes, fundador, diretor-executivo e auditor-líder da AIRJOB Auditores e Consultores, "*risco zero é impossível para qualquer ser vivo!*"

Partindo desta premissa, a existência de um plano de respostas a incidentes - PRI robusto é o diferencial para que a organização esteja preparada para lidar com vazamentos de dados, garantindo a proteção dos dados de titulares e evitando sanções administrativas.

O PRI deve fornecer instruções que auxiliem a identificar se um determinado incidente de segurança é também um vazamento de dados, ou seja, se o incidente detectado acarreta risco ou dano relevante aos titulares de dados, sendo de acordo com o art.48 da LGPD, necessário comunicar à ANPD e aos titulares dos dados sobre o incidente identificado.

Considerando as boas práticas identificadas, a Connect Point estabeleceu em seu Plano de Respostas à Incidentes:

a. instruções para garantir o sigilo de informações sensíveis quanto ao vazamento;
b. definição de funções e responsabilidades de unidades organizacionais durante o vazamento;
c. escalonamento de possíveis problemas e relato de atividades suspeitas;
d. classificações de gravidade de incidentes;

e. orientações para comunicações externas.

4.7.3. Design

Considerando que a Connect Point não possui nenhum profissional especialista em segurança da informação, foi estabelecida uma parceria com uma empresa especialista em segurança cibernética, na qual em reuniões para apresentação do modelo de negócio, foram apontadas possibilidades de ameaças que poderiam comprometer a segurança dos dados tratados, além da realização de uma modelagem detalhada de todo fluxo de tratamento de dados, caracterizando a forma mais segura para desenvolvimento das funções, seja para acessos internos ou externos.

Como base no direcionamento das ações, foi utilizado como referência as recomendações da *European Union Agency for Network and Information Security* – ENISA[49] e separando os requisitos orientados à dados e os requisitos orientados à processos.

Com relação aos requisitos orientados à dados, são consideradas 5 (cinco) avaliações estratégicas como boa prática a ser utilizada:

i. **Minimize e limite**: assim como já definido pelo art. 6º, III, a ENISA orienta que a quantidade de informações pessoais coletadas e processadas, precisa ser limitada àquelas que são legais e estritamente necessárias nas diretrizes de *Privacy by Design*. Os dados devem ser deletados quando seu armazenamento não for mais exigido para seus propósitos.
ii. **Esconda e proteja**: os dados pessoais e as formas com que elas se relacionam não devem ser comunicadas, processadas ou armazenadas diretamente à vista. Ao esconder dados pessoais facilmente identificáveis, o risco de abuso e o escopo de acidentes em potencial são

[49] Material disponível para consulta em: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/@@download/fullReport, acessado em 04/03/2022.

significativamente reduzidos. Como mecanismos técnicos, são sugeridas soluções de pseudonimização[50] ou a criptograma[51].

iii. **Separe**: Ao separar o processamento ou o armazenamento de diversas fontes de dados pessoais que pertencem a um mesmo indivíduo, é possível diminuir as possibilidades de que seja possível criar um perfil completo de um titular. Esta prática orienta que de acordo com cada propósito, a informação deve ser armazenada em bases de dados distintas, dificultando que diferentes conjuntos de dados possam ser relacionados entre si.

iv. **Agrege**: Para garantir a proteção dos direitos dos titulares em relação a seus dados pessoais, eles devem ser colhidos e processados com o maior nível de agregação quanto possível. Esta prática sugere evitar ao máximo o detalhamento de informações particulares nas limitações daquilo que ainda pode ter valor para o seu negócio e faça sentido para os propósitos de coleta e de uso.

v. **Proteção de dados como padrão**: Recomenda-se que todas as configurações devem vir por padrão em suas formas mais "*privacy-friendly*". Desta forma, o usuário terá que fazer uma escolha consciente se optar por mudar qualquer configuração que resulte em uma configuração menos amigável à privacidade como por exemplo compartilhar mais dados com outras pessoas.

Considerando os requisitos orientados à projetos, são consideradas 4 (quatro) avaliações estratégicas como boa prática a ser utilizada:

i. **Informe**: Assim como estabelecido no princípio da finalidade descrito no art. 6º, I, esta orientação estabelece que o programa deve ser desenhado e configurado de forma que o titular tenha informações suficientes sobre como o software funciona e sobre como seus dados pessoais são processados. Havendo a modelagem de dados de forma à viabilizar o estabelecimento de perfis ou mesmo automatizar a tomada de decisões a

[50] Pseudonimização consiste em técnicas de 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.

[51] Criptograma refere-se à construção e análise de protocolos que impedem terceiros, ou o público, de lerem mensagens privadas.

partir de dados pessoais, o titular precisa saber como este processo é realizado, assim como atendendo o que é estabelecido no art. 20, § 1º.

ii. **Controle**: Atendendo ao princípio de livre acesso previsto no art. 6º, IV, esta prática recomenda que o indivíduo detentor dos dados, ou seja, o titular, tem o direito de controle sobre suas próprias informações pessoais. Isso inclui o direito de acessar, atualizar e/ou deletar esses dados. O design do programa deve garantir que o cliente possa exercer esses direitos o mais facilmente possível.

iii. **Reinforce**: O software deve ser projetado de modo a documentar como está prevista a exigibilidade dos direitos do titular dos dados. A documentação deve abranger a responsabilidade e como o regulamento de proteção de dados é aplicado. Deve estar disponível para auditorias e inspeções do processamento, incluindo também inteligência artificial, perfis e processamento automatizado.

iv. **Demonstre**: O controlador precisa ser capaz de documentar os processos de *compliance* relacionados à proteção de dados e à segurança do processamento. A aplicação deve ser projetada e desenvolvida para que o controlador possa documentar e demonstrar como os requisitos da proteção de dados foi implementada.

4.7.4. Testes

Visando garantir condições mais favoráveis em relação à segurança e privacidade, foi estabelecida uma rotina para validar e testar se os requisitos de proteção e segurança não somente estão implementados como também se estão implementados de forma eficiente, inclusive nos ambientes de testes.

Como o apoio do parceiro de segurança cibernética, foram estabelecidas rotinas de testes dinâmicos, testes de *fuzzing* e testes de penetração.

Nos testes dinâmicos, foram testadas as funcionalidades do código da plataforma de associação de profissionais diante de vários cenários de permissões de acesso, sistemas operacionais e dispositivos com o intuito de identificar falhas de segurança por meio de tentativas de acessos indevidos. Após cada rotina de testes,

os resultados foram tabulados e comparados à outros testes em ambientes diferentes. Estes testes foram responsáveis por garantir que os usuários só terão acesso às informações e funcionalidades para as quais foram estabelecidas na definição do perfil.

Nos testes de *fuzzing*, foram elaboradas bases de dados com diferentes formatos, duplicidades, inconsistências e até mesmo com partes de códigos em *javascript*[52], buscando forçar comportamentos inesperados da ferramenta tais como alteração e eliminação de tabelas, realização de *looping* infinito[53] em consultas e transferências do conteúdo do banco de dados.

Por último, a sequência de testes que envolveu maior esforço técnico, foram as análises de vulnerabilidade e teste de penetração. Para este momento, foram realizadas rotinas de identificação de falhas e vulnerabilidade que pudessem expor a plataforma à diferentes tipos de ameaças. Muitas vezes, estas fragilidades de segurança acontecem por falhas humanas, erros de programação ou má configuração da infraestrutura.

As falhas humanas são comuns de acontecer, principalmente com colaboradores sem treinamento, que clicam em links suspeitos ou baixam documentos infectados, por exemplo.

Os erros de programação se dão por falhas nos desenvolvimentos de sistemas que mantêm brechas que podem atrair vulnerabilidades, enquanto a má configuração são os softwares sem devida manutenção, que não garantem uma segurança adequada.

A análise de vulnerabilidades tem diversos objetivos além de identificar e corrigir brechas nos sistemas, e podemos citar o desempenho e segurança, a melhoria da configuração dos softwares, implantação de novas soluções de segurança, garantir a melhoria contínua de infraestrutura da empresa, entre outros.

---

[52] *JavaScript* é uma linguagem de programação de alto nível criada, a princípio, para ser executada em navegadores e manipular comportamentos de páginas web.

[53] Looping infinito é uma sequência de instruções em um programa de computador que repete infinitamente, ou porque não há condição de parada ou porque a condição existe, mas nunca é atingida.

Na primeira avaliação realizada, embora não tenha sido identificado risco com criticidade alta, foram identificados 9 outros tipos de ricos:

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	4
Informational	2

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	7
Missing Anti-clickjacking Header	Medium	6
Vulnerable JS Library	Medium	3
Cookie Without Secure Flag	Low	2
Cross-Domain JavaScript Source File Inclusion	Low	8
Timestamp Disclosure - Unix	Low	19
X-Content-Type-Options Header Missing	Low	37
Information Disclosure - Suspicious Comments	Informational	48
Re-examine Cache-control Directives	Informational	7

Figura 12 - Resultado da análise gerada pelo OWASP ZAP[54]
Fonte: *Elaborado pelo autor*

Após a realização do *scan* de vulnerabilidades, foram realizados testes de invasão com o intuito de testar a segurança do portal. No teste de penetração, ou simplesmente *pentest*, é um conjunto de técnicas e ferramentas utilizadas para identificar falhas de segurança em sistemas e redes corporativas, simulando ações de *hackers* e criminosos para infiltrar a estrutura de TI.

No modelo utilizado junto à Connect Point, foi realizada uma simulação de ataque tipicamente externo, levando em consideração que o *hacker* não conhece a infraestrutura utilizada. Este modelo é denominado *black box*. Existem também outros tipos de simulações que são o *white box,* que simula o ataque de um *hacker* já tem conhecimento da infraestrutura analisada, identificando atividades que são feitas de dentro da empresa ou por pessoas que conhecem os sistemas e o *grey box*, que é um teste intermediário, que mistura o *black box* e o *White box*, ou seja, simula uma

[54] OWASP ZAP é um scanner de segurança de aplicativos da web de código aberto. Ele deve ser usado tanto por aqueles que são novos em segurança de aplicativos quanto por testadores de penetração profissionais. É um dos projetos mais ativos do Open Web Application Security Project e recebeu o status de carro-chefe.

situação na qual o *hacker* tem algumas informações, mas não sabem tudo sobre a infraestrutura.

4.7.5. Manutenção

Com toda a base estruturada e reconhecendo os pontos fortes e fracos do modelo da *startup*, agora é o momento de buscar mecanismos para manter fortalecida toda a estrutura construída por quase dezoito meses, vivenciando erros e acertos, críticas e elogios.

Um dos fundamentos de maior importância em todo processo do *Privacy by Design*, é a necessidade de segurança forte, de ponta a ponta, com proteção total do ciclo de vida e para isso o envolvimento de todos da equipe torna-se de fundamental importância.

Considerando que os processos são contínuos, tanto do ponto de vista de criação como também da maturidade, estabelecer uma rotina de reavaliação de todo modelo aplicado é o que irá proporcionar a continuidade da privacidade, mantendo este princípio incorporado ao produto e serviço.

5. CONSIDERAÇÕES FINAIS

Diante dos vários desafios de uma *startup*, a partir de agosto de 2020 estas empresas em estágio de desenvolvimento se deparam com a necessidade de adequação à Lei Geral de Proteção de Dados, frente à um cenário de crise proporcionado pela pandemia de COVID-19.

Considerando o caráter inovador das *startups* e também sua característica de rápida adaptação às mudanças, é importante identificar este como um cenário de oportunidades e buscar alternativas práticas e funcionais para adequar à esta nova realidade.

Oferecer um produto robusto e confiável é proposta de valor para qualquer empreendimento e isso não é diferente para uma *startup*. A necessidade de se adequar à LGPD trouxe para as empresas uma grande oportunidade de descobrir suas vulnerabilidades tanto no ambiente físico como no digital, uma vez que a adequação começa pela avaliação e mitigação das lacunas de segurança identificadas. Para uma *startup*, apresentar-se ao mercado com o modelo de privacidade já mapeado e controlado, certamente trata-se de um diferencial competitivo, e nestes casos, nada mais coerente do que pensar na privacidade desde a criação do projeto.

O *Privacy by Design*, foi a metodologia mais adequada ao momento da Connect Point, uma vez que com ele foi possível controlar o ambiente de tratamento de dados de forma satisfatória ao que está estabelecido pela legislação. Com este modelo, foi possível adotar todas as medidas possíveis para proporcionar um ambiente mais seguro para os clientes seja considerando a plataforma desenvolvida, o modelo de negócio e o ambiente de infraestrutura organizado para suportar todo o negócio.

Financeiramente, o investimento realizado para a implantação do *Privacy by Design* não representou impactos significativos no orçamento da Connect Point uma vez que grande parte do *know how* envolvido estava internalizado na *startup*, sendo necessário apenas o aperfeiçoamento e o direcionamento teórico.

Embora o *Privacy by Design* tenha contribuído para o adiamento da data de lançamento da plataforma aos clientes em mais de 3 meses, é importante ressaltar

que após a aplicação da metodologia os clientes terão uma plataforma mais segura, garantindo todos os direitos dos titulares de dados previstos pela Lei Geral de Proteção de Dados – LGPD, representando com isso, grande vantagem comercial.

O *Privacy by Design*, é um conceito diferenciado pois além de proporcionar a privacidade propriamente dita, é responsável por aumentar a qualidade e a percepção de segurança das pessoas.

Como sugestão de novos estudos relacionados ao tema, é importante avaliar como as *startups* que utilizaram o *Privacy by Design* se posicionaram no mercado após o primeiro ano de atividade. Esta avaliação pode ser realizada também considerando empresas já estabelecidas no mercado, após a utilização do *Privacy by Design* e *Privacy by Default* para a adequação à LGPD.

REFERÊNCIAS BIBLIOGRÁFICAS

AL-FEDAGHI S.S. (2007) The “Right to be let alone” and private information. In: Chen CS., Filipe J., Seruca I., Cordeiro J. (eds) Enterprise Information Systems VII. Springer, Dordrecht. Disponível em: https://doi.org/10.1007/978-1-4020-5347-4_18, acessado em 13/02/2022.

ALAN F. Westin, Privacy And Freedom, 25 Wash. & Lee L. Rev. 166 (1968). Disponível em https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20, acessado em 03/05/2022.

ALEXY, Robert. Teoria de los derechos fundamentales. Trad. Ernesto Garzón Valdés. Madri: Centro de Estudos Constitucionales, 1993.

ASSOCIAÇÃO BRASILEIRA DE STARTUPS - Manual sobre conceitos, metodologias e investimentos em startups, 2014. Disponível em: https://www.abstartups.com.br. Acessado em: 27/01/2022.

BARATI, Masoud; RANA, Omer; PETRI, Ioan; THEODORAKOPOULOS, George. GDPR Compliance Verification in Internet of Things, IEEE Access, vol.8, p. 119697 – 119709, Junho 2020.

BASAN, A. P.; FALEIROS JÚNIOR, J. L. DE M. A proteção de dados pessoais e a concreção do direito ao sossego no mercado de consumo. civilistica.com, v. 9, n. 3, p. 1-27, 22 dez. 2020.

BELLER, Jonathan. Digitality and the media of dispossession. In: SCHOLZ, Trebor. Digital labor: the internet as playground and factory. Nova Iorque; Londres: Routledge, p. 213-236, 2013.

BRASIL. Diário oficial da união, Rio de Janeiro, RJ, Disponível em https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019, acessado em 17/03/2022.

BRASIL. Lei nº 13.709, de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm, acessado em 13/01/2022.

BREITBARTH, Paul (2019), The impact of GDPR one year on, Network Security, Vol. 2019, P. 11-13, Julho 2019.

BRENNER, Susan W. Constitutional rights and new technologies in the United States. In: LEENES, Ronald; KOOPS, Bert- Jaap; DE HERT, Paul. Constitutional rights and new technologies – A comparative study. Tilburg: T.M.C. Asser Press, 2008.
CHEMERINSKY, Erwin. Constitutional law – Principles and policies. 3. ed. New York: Aspen Publishers, 2006.

COELHO, C. F., Rasma, E. T., & Morales, G. (2013). ENGENHARIA SOCIAL: UMA AMEAÇA À SOCIEDADE DA INFORMAÇÃO. Exatas & Engenharias, 3(05), disponível em https://doi.org/10.25242/885X305201387, acessado em 02/02/2022.

COOPER, D. R.; SCHINDLER, P. S. Métodos de pesquisa em Administração. 7 ed. Porto Alegre: Bookman, 2003.

DÖHMANN, Indra Spiecker Gen. A proteção de Dados Pessoais sob o Regulamento Geral de Proteção de Dados na União Europeia.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). Tratado de Proteção de Dados Pessoais. 1º ed. Rio de Janeiro: Forense, 2021. pp. 16-17, 97-98.

FORBES. How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. Disponível em: <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girlwas-pregnant-before-her-father-did/>. Acessado em 02/04/2022

FRAZÃO, Ana. A proteção de dados pessoais em tempos de pandemia: A MP 959 e o preocupante adiamento da entrada em vigor da LGPD. Disponível em:

https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/a-protecao-de-dados-pessoais-em-tempos-de-pandemia-01052020, acessado em 17/01/2022.

GAVISON, Ruth. Privacy and the Limits of the Law. Yale Law Journal, 1980, 89.

HENDRICKS, Evan; HAYDEN, Trudy; Novik, Jack D. Your right to privacy: a basic guide to legal rights in an information society. 2. ed. Chicago: Southern Illinois University Press, 1990.

HUFFPOST, 2017. Facebook's Zuckerberg Says Privacy No Longer A Social Norm. Disponível em: https://www.huffpost.com/entry/facebooks-zuckerberg-the_n_417969, acessado em 03/04/2022.

IDEC, 2020. Após denúncia do Idec, Hering é condenada por uso de reconhecimento facial. Disponível em: https://idec.org.br/noticia/apos-denuncia-do-idec-hering-e-condenada-por-uso-de-reconhecimento-facial, acessado em 03/04/2022.

INNESS, Julie C., Privacy, intimacy and isolation 3 (1992).

JOURARD, Sidney M. Some Psychological Aspects of Privacy, 31 Law & Contemp. Probs. 307, 307 (1966)

LINDEN, Thomas; KHANDELWAL, Rishabh; HARKOUS, Hamza e FAWAZ, Kassem. The Privacy Policy Landscape After the GDPR. Proceedings on Privacy Enhancing Technologies, Poland, Journal volume & issue, v.2020, n. 1, p. 47- 64, janeiro 2020

MAGRANI, Eduardo. Entre dados e robôs: ética e privacidade na era da conectividade. 2 ed. Porto Alegre: Arquipélago Editorial, 2019

O’BRIEN, David M. Privacy, Law, and Public Policy – Publicado em 15 de Julho de 1979, Praeger

POSNER, Richard A. The Economics of Justice 272-73 (1981).

QUELHAS, O. L. G.; FILHO, J. R. F.; FRANÇA, S. L. B. O mestrado profissional no contexto do sistema de pós-graduação brasileiro. Revista Brasileira de Pós-Graduação, v. 2, n. 4, 11.

Revista Governança e Compliance ACRJ, Edição 8 – Ano 4 – Abril, 2021. Associação Comercial do Rio de Janeiro, disponível em: https://acrj.org.br/wp-content/uploads/2021/04/revista_governanca_compliance_abr_2021_12_04.pdf, acessado em 17/02/2022.

STANLEY I. Benn. Privacy, freedom, and respect for persons. Published online by Cambridge University. December 2009 - Edited by Ferdinand David Schoeman

TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. civilistica.com, vol. 9, n. 1, p. 1-38, 9 maio 2020

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Lei Geral de Proteção de Dados Pessoais: Artigo comentado. Salvador: Editora JusPodivm, 2019

YIN, Robert K. Estudo de Caso: Planejamento e métodos. Bookman editora, 2015.