



Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito

REBECCA DE ARAUJO FROIS

**LGPD: MECANISMOS DE SEGURANÇA, DA INVASÃO À PROTEÇÃO DE
DADOS**

**TAGUATINGA
2021**

REBECCA DE ARAUJO FROIS

LGPD: MECANISMOS DE SEGURANÇA, DA INVASÃO À PROTEÇÃO DE DADOS

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Leonardo Gomes de Aquino

**TAGUATINGA
2021**

REBECCA DE ARAUJO FROIS

LGPD: MECANISMOS DE SEGURANÇA, DA INVASÃO À PROTEÇÃO DE DADOS

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Leonardo Gomes de Aquino

TAGUATINGA, dia de outubro de 2021.

BANCA AVALIADORA

Professor Orientador Leonardo Gomes de Aquino

Professor(a) Avaliador(a)

Dedico esse trabalho a Deus, ao tempo, às oportunidades que a vida nos apresenta, às oportunidades criadas por mim, às minhas filhas Larissa e Sophia e ao meu esposo Bruno.

AGRADECIMENTOS

A trajetória até aqui foi longa, muitos aprendizados, experiências que levarei comigo por toda a vida. Agradeço aos birôs de crédito existentes no país, em especial aqueles em que tive a honra de trabalhar e aprender sobre a proteção e a ciência de dados: Serasa Experian e Boa Vista SCPC. Serei eternamente grata aos ensinamentos transmitidos pelos meus clientes e parceiros comerciais, em cada visita, reunião, workshop, enfim em cada momento que tive a oportunidade de aprender sobre a realidade de cada empresa.

Agradeço aos professores que contribuíram para a minha maturidade acadêmica e pessoal, em especial para os professores Leonardo Aquino e Carolina Costa que mostraram o caminho para um trabalho acadêmico dentro das normas acadêmicas abordando como o direito impacta diretamente a vida, os dados, as relações e a experiência dos indivíduos.

Meus sinceros agradecimentos a todas as pessoas que participaram da pesquisa e que trouxeram um novo olhar para o entendimento da proteção de dados, conseqüentemente para esse trabalho, em especial para o entendimento da LGPD hoje.

RESUMO

Este trabalho de conclusão de curso busca estabelecer quais são os melhores procedimentos para adequação da base de clientes atual das empresas à LGPD – Lei Geral de Proteção de Dados, assim como compartilhar boas práticas neste caminho de adequação. Considerando o tempo e nível de complexidade para a adequação de todas as pessoas físicas e jurídicas quanto a nova legislação no Brasil, o estudo foi centralizado em como as empresas devem se adequar, utilizando como embasamento legal a legislação vigente e pesquisas com empresas e com pessoas físicas estabelecendo o caminho a ser seguido, e quais são os mecanismos de segurança necessários e recomendados para realização do tratamento de dados pessoais de clientes e empregados nas empresas. Buscou-se estabelecer um processo de governança de dados para que os portadores de bases de dados possam atender a legislação de forma contínua, mais rápida, eficiente e com baixo custo. E desta forma prevenindo a invasão e divulgação de dados dos titulares. Foram utilizados o método dedutivo, apresentando premissas para definição, utilizou-se a pesquisa bibliográfica, pesquisa empírica para o mapeamento dos direitos e responsabilidades que as pessoas físicas e pessoas jurídicas possuem assim como estruturar formas de comunicação e de adequação à legislação vigente.

Palavras-chave: Lei Geral de Proteção de Dados; Proteção de Dados Pessoais; Privacidade; Autoridade Nacional de Proteção de Dados; Direito Digital.

SUMÁRIO

INTRODUÇÃO	7
1 DA INVASÃO A PROTEÇÃO DE DADOS	11
1.1 Da Invasão.....	12
1.2 Proteção de Dados	16
1.2.1 <i>Da Propriedade do Dado</i>	18
2 DA REALIDADE NAS EMPRESAS.....	20
3 DA LEGISLAÇÃO VIGENTE.....	29
3.1 União Européia.....	30
3.2 Estados Unidos da América	31
3.3 América Latina	33
4 POLÍTICAS PÚBLICAS	35
CONCLUSÃO	54
REFERÊNCIAS.....	57

INTRODUÇÃO

É sabido que a Revolução Industrial foi um marco na evolução da sociedade, e desde então a tecnologia e o domínio dela refletem em controle e poder. Até hoje, as tomadas de decisão de quem detém o poder são estrategicamente elaboradas considerando informações, estatísticas, modelos preditivos, dados, comportamentos e imagem. E através destas informações é possível prever cenários, criar uma reputação, reverter situações, falar diretamente com o perfil do público estabelecido, utilizando a mesma linguagem, além de desenvolver a melhor estratégia e forma para influenciar determinado grupo de pessoas.

A Lei Geral de Proteção de Dados (LGPD)¹, é uma lei recente, Lei 13.709/2018. A norma estabelece que empresas, assim como órgãos públicos considerando o âmbito federal, estados e municípios só poderão armazenar dados pessoais com a permissão do titular. Atualmente, em muitas situações, esses dados pessoais são capturados pela internet e vendidos, assim como os perfis de acordo com o interesse do comprador de informações.

Tendo em vista a adequação de todas as pessoas físicas e jurídicas quanto à nova legislação; a LGPD é uma norma efetiva para a proteção de dados pessoais, regulamentando mecanismos de segurança, evitando a invasão dos Banco de Dados e a utilização indevida?

As empresas que não atenderem a LGPD, estão vulneráveis e sujeitas a falhas de segurança, e podem ser penalizadas com sanções administrativas inclusive multas de até R\$50 milhões. A lei entrou em vigor, as sanções administrativas começaram em 1º de agosto de 2021. Neste contexto ainda não está claro por onde devem iniciar a adequação a legislação vigente para muitos segmentos. A Autoridade Nacional de Proteção de Dados Pessoais (ANPD) é a responsável por regular, orientar e aplicar a

¹ BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 10 jan. 2021.

lei, com a colaboração de cidadãos e organizações, no entanto, ainda faltam definições legais sobre a ANPD.

Assim, entrelaçamos a norma vigente com a realidade das empresas e deste modo conseguimos estabelecer quais são os melhores procedimentos, por onde começar para adequar a base de clientes atual das empresas à LGPD. Assim como sugerir um processo de governança de dados para que as empresas do mercado possam atender a legislação vigente de forma contínua, mais rápida, eficiente e com baixo custo.

Trata-se de um tema relevante, atual e que está em evidência no que tange às questões de captura, armazenamento e tratamento de dados, é uma lei que estabelece níveis de segurança inclusive corresponde a uma etapa referente a norma do marco legal da lei da internet onde os dados pessoais são capturados e na maioria das vezes sem o consentimento do titular. As análises serão estruturadas e apresenta uma sugestão para informar às pessoas que a empresa precisa do dado pessoal e como esses serão utilizados.

O objetivo geral deste trabalho é analisar e estabelecer os cuidados necessários para adequar a empresa a LGPD, quais são os mecanismos de segurança eficientes na realização de tratamento e armazenamento de dados pessoais.

Os objetivos específicos são: Analisar as adequações que as empresas já fizeram, e realizar um paralelo sobre como deverão se adequar para atender a legislação vigente; Estabelecer quais são os mecanismos de segurança necessários e recomendados para realização do tratamento de dados pessoais de clientes e funcionários nas empresas; Comparar a Lei Geral de Proteção de Dados com outras legislações que tratam da proteção de dados, assim como a privacidade dos dados pessoais e investigar o nível de entendimento que a população e as empresas têm sobre seus direitos e responsabilidades quanto a instituição da Lei Geral de Proteção de Dados.

Os temas estão distribuídos da seguinte forma: O primeiro capítulo reserva-se para falarmos da Invasão a Proteção de dados, e de como os dados atualmente são vulneráveis. No segundo capítulo, iremos identificar, consolidar e criticar as deficiências das empresas. Já no terceiro capítulo, abordamos a base legal para a proteção dos dados pessoais no direito brasileiro. Consideramos a diferença da norma brasileira e outras normas, os padrões estabelecidos na norma e as lacunas da norma onde proponho soluções. No quarto capítulo, temos um panorama de ideias para políticas públicas para pessoas físicas.

Abordaremos de forma metodológica realizando um contraponto de cada tópico com a norma, estruturando assim uma forma de proteção de dados e do reflexo da utilização indevida na vida e no direito dos brasileiros.

Será utilizado o método dedutivo, apresentando premissas para definição. Quanto à metodologia utilizou-se a pesquisa bibliográfica, pesquisa empírica para o mapeamento dos direitos e responsabilidades que as pessoas físicas e pessoas jurídicas possuem atualmente e estruturar formas de comunicação e de adequação à legislação vigente.

Foi utilizado um recorte temporal de 6 meses de 1º/12/2020 a 1º/06/2021 pois assim conseguimos um volume maior de retorno com um recorte temporal de 180 dias, com objetivo de obter 30% de respostas nos questionários disponibilizados tanto para as pessoas físicas quanto para as pessoas jurídicas. As entrevistas com os bureaus de crédito² foram realizadas de 1º/07/2021 a 30/09/2021.

Será possível analisar as adequações que as empresas já realizaram, e realizar um paralelo sobre como deverão se adequar para atender a legislação vigente, o que falta, como facilitar a transição, como evitar sanções através de consultoria e

² De acordo com a ANBC, bureaus de crédito fazem a ponte entre quem quer comprar a crédito e que vende produtos e serviços. ANBC. **Associação Nacional dos Birôs de Créditos**. <https://anbc.org.br/o-que-e-um-biro-de-credito/>. Acesso em: 01 out. 2021.

capacitação dessas empresas. Iremos estabelecer quais são os mecanismos de segurança necessários e recomendados para realização do tratamento de dados pessoais de clientes e funcionários nas empresas, assim como realizar uma crítica construtiva à forma de divulgação da nova legislação e propor novos meios de comunicação aos cidadãos sobre os direitos e deveres.

Deste modo, realizamos uma comparação da Lei Geral de Proteção de Dados com outras legislações que tratam da proteção de dados, assim como a privacidade dos dados pessoais, inclusive de legislações vigentes em outros países. Assim irei propor em um formato simples e objetivo os mecanismos de segurança tanto para as empresas quanto para os cidadãos sobre segurança da informação e como se adequar a legislação vigente, evitando assim a invasão de dados.

1 DA INVASÃO A PROTEÇÃO DE DADOS

Até um determinado momento histórico, a tutela jurisdicional sobre a privacidade, liberdade e igualdade foi suficiente. Devido a novos desdobramentos da era moderna, reacenderam a necessidade de novos limites, já adaptados à realidade da era digital. Ao longo dos anos, aconteceram diversas situações que influenciaram para o surgimento de uma normativa que zela pela proteção dos dados.

Quando o assunto é a invasão de dados, de acordo com cada situação existe a violação de vários princípios constitucionais, e entre eles a violação do direito à privacidade. O direito à proteção dos dados pessoais é uma das violações da invasão, sejam através da divulgação ou utilização sem o consentimento do “dono do dado”, e como exemplo cito dados pessoais, fotografias, imagens, dados bancários, documentos, entre outros.

Tristan Harris, executivo do Google, faz um alerta sobre as facilidades e os riscos que as redes sociais nos trouxeram. Sendo que o impacto maior é sobre a democracia e a humanidade tendo em vista que não foram mapeadas as reações do uso indevido e do abuso na utilização. Sem dúvidas, um risco alto para os dados pessoais que tramitam no ambiente online.

Especialistas em tecnologia e profissionais da área fazem um alerta: as redes sociais podem ter um impacto devastador sobre a democracia e a humanidade. As redes sociais trouxeram muitas facilidades no mundo moderno, no entanto, não foram mapeadas as reações adversas que poderiam causar o uso indevido ou abuso na utilização, até mesmo possíveis utilizações perigosas. “Nada grandioso entra nas vidas dos mortais sem uma maldição”. “Saímos da era da informação para entrar na era da desinformação. Tristan Harris (Google Former Design Ethicist)” 5’28” – 5’30”³

Hoje, além dos vazamentos de dados que ocorrem nas grandes instituições, a sociedade tem a preocupação com a invasão dos dados nos acessos realizados por computadores para uso doméstico. Com a era da informação, e a facilidade que a

³ O DILEMA das Redes. Diretor Jeff Orlowski /produtora Larissa Rhodes. **Netflix**, 2020. Tristan Harris (Google Former Design Ethicist)” 5’28” – 5’30”.

internet proporcionou a sociedade, carregamos o ônus da vulnerabilidade de nossos pontos de acesso à internet, seja através de um notebook, um celular, um tablet, uma TV smart, um computador, entre outros.

1.1 Da Invasão

A invasão de bancos de dados ou até mesmo o vazamento destas informações acarretam inúmeros transtornos para a sociedade e para as empresas. A indústria da tecnologia enumera escândalos com vazamentos de dados e sanções aplicadas às empresas. E com isso a busca por uma normatização, uma forma de proteção dos dados é o mínimo que as pessoas de boa-fé almejam.

Ao perguntarmos às pessoas qual é o problema da indústria da tecnologia, haverá uma cacofonia de queixas e escândalos, sobre o roubo de dados, vício em tecnologia, além das fakenews, da polarização e da influência nas eleições. Mas será que existe uma raiz para todos esses problemas, algo que faz com que tudo isso aconteça ao mesmo tempo? – Tristan Harris (Google Former Design Ethicist) 06'10" – 6'41".⁴

Em 1890, o artigo jurídico *The Right to Privacy*⁵ de Samuel Warren e Louis Brandeis é amplamente conhecido nos Estados Unidos como a primeira publicação do país a defender o direito à privacidade.

Warren e Brandeis consideram a proteção do *privacy* uma necessidade: "*The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.*"

⁴ O DILEMA das Redes. Diretor Jeff Orlowski /produtora Larissa Rhodes. **Netflix**, 2020. Tristan Harris (Google Former Design Ethicist)" 06'10" – 6'41".

⁵ WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890.

Dentre os gigantes das redes sociais, em sua maioria, todos possuem admiração mútua, não apenas pelo serviço prestado, mas também pelo volume em bilhões de dólares que essas empresas movimentam todos os anos, com um “produto” que não é de propriedade ou exclusividade de determinada rede social, ou seja, com os dados pessoais. A rede social não é “dona do dado”, e mesmo ganhando muito dinheiro com a utilização de informações da população, toma medidas para que o seu legado se mantenha crescente no mercado.

Todo o mundo em 2006, incluindo nós no facebook, tinham total admiração pelo Google e pelo que ele construiu. Um serviço incrivelmente útil, que tinha gerado, até onde percebíamos, muita coisa boa para o mundo e que, em paralelo, era uma máquina de ganhar dinheiro. - Tim Kendall (Facebook former executive/Pinterest former presidente/moment CEO)” 10’35” – 10’59”⁶

O principal insumo das gigantes redes sociais é o dado. Hoje é um grande negócio vender anúncios para empresas com a certeza de atingir o público-alvo de determinada campanha. São utilizados dados, modelos preditivos para que possam fazer com que determinada informação chegue a um perfil de público específico.

As empresas Facebook, Snapchat, Twitter, Instagram, Youtube, Tiktok, Google, Pinterest, Reddit e LinkedIn possuem o modelo de negócios voltado a manter das pessoas conectadas à tela. “Esse é o sonho de qualquer negócio. Ter a garantia de que o anúncio publicado será bem sucedido. Esse é o negócio dessas empresas. Elas vendem a certeza. Para ter sucesso nesse negócio, é preciso fazer grandes previsões assertivas. Para isso, existe um fator fundamental. Você precisa de muitos dados. - Shoshana Zuboff, PhD (Harvard Business School Professor Emeritus/Author The Age of Surveillance Capitalism)” 15’00” - 15’26”⁷

Tudo que fazemos na internet, é monitorado. Cada ação, cada imagem que observamos e quanto tempo observamos. Eles têm mais informações sobre nós do

⁶ O DILEMA das Redes. Diretor Jeff Orlowski /produtora Larissa Rhodes. **Netflix**, 2020. Tim Kendall (Facebook former executive/Pinterest former presidente/moment CEO)” 10’35” – 10’59””.

⁷ O DILEMA das Redes. Diretor Jeff Orlowski /produtora Larissa Rhodes. **Netflix**, 2020. Shoshana Zuboff, PhD (Harvard Business School Professor Emeritus/Author The Age of Surveillance Capitalism)” 15’00” - 15’26”.

que já imaginaram na história da humanidade. Algumas pessoas acreditam que os nossos dados são vendidos, mas de fato são construídos modelos preditivos de nossas ações e quem tem o melhor modelo é mais assertivo nas ofertas dos anunciantes.

Eles constroem modelos que preveem nossas ações, e quem tiver o melhor modelo, vence. [...] do outro lado da tela é quase como se tivessem um boneco de vodu de nós. Tudo que já fizemos, os cliques que já demos, os vídeos que assistimos, as curtidas, tudo isso ajuda a moldar um modelo cada vez mais fiel. Assim que o modelo é criado, é possível prever um padrão de comportamento. – Tristan Harris (Google Former Design Ethicist)” 17’50” - 18’29”⁸

Com o modelo é possível prever aonde a pessoa quer ir, qual vídeo irá te manter conectado, prevê que tipo de emoções pode sensibilizar a pessoa. No ambiente online as pessoas ganham novas personalidades, e a exposição dos dados, das opiniões, das reações fazem parte do arcabouço de informações que são capturadas pela internet desde muito antes da lei de proteção de dados no planeta.

Em muitas dessas empresas de tecnologia, há três objetivos principais. O objetivo de engajamento, para aumentar o seu uso, e te manter navegando. O de crescimento, para que você retorne e sempre convide amigos e faça com que eles convidem mais amigos e a meta da propaganda, para garantir que enquanto tudo acontece, as empresas estejam lucrando o máximo possível com anúncios. – Tristan Harris (Google Former Design Ethicist)” 18’56” - 19’18”⁹

Em uma entrevista Edward Tufte afirma que existem apenas duas indústrias que chamam seus clientes de usuários: a de drogas e a de software. Neste sentido podemos concluir muitas questões de como determinadas pessoas conseguem passar tanto tempo conectados e como o desejo aumenta cada vez mais pela utilização.

Se as redes sociais nos manipulam e preveem nossos hábitos de consumo e até mesmo emoções, isso impacta diretamente a nossa saúde mental, assim como o tempo que é gasto diariamente com o uso das redes sociais. “Existem apenas duas indústrias que chamam

⁸ O DILEMA das Redes. Diretor Jeff Orlowski /produtora Larissa Rhodes. **Netflix**, 2020. Tristan Harris (Google Former Design Ethicist)” 17’50” - 18’29.

⁹ O DILEMA das Redes. Diretor Jeff Orlowski /produtora Larissa Rhodes. **Netflix**, 2020. Tristan Harris (Google Former Design Ethicist)” 18’56” - 19’18”.

seus clientes de usuários: a de drogas e de software. – Edward Tufte”(Emeritus Professor of Statistics, graphic design, and political economy at Yale University) 30’49 – 30’55”¹⁰

O nível de persuasão das redes sociais tendo como base nossos dados pessoais e comportamentais tornam as pessoas vulneráveis, e expostas a propagandas, ideias, tendências políticas além de outras vulnerabilidades.

Se eu quiser manipular uma eleição, posso ir a um grupo de teoria da conspiração no facebook e encontrar cem pessoas que acreditam que a Terra é plana e que o homem nunca pisou na lua. Então, posso pedir ao facebook que me mostre mil usuários daquele tipo. O facebook me mostrará tais usuários com aquele perfil, propensos a acreditar em uma nova teoria da conspiração. – Tristan Harris (Google Former Design Ethicist)” 1’08”27 – 1’08”54¹¹

Peço vênia, para adentrar em uma questão política. Tivemos inclusive um candidato eleito, que movimentou sua campanha 100% pelas redes sociais no Brasil.

As eleições no Brasil foram fora do comum. Foi uma campanha impulsionada pelas mídias sociais. Nós da indústria da tecnologia criamos ferramentas, que desestabilizam e destroem o equilíbrio da sociedade, em todos os países, de uma vez. – Tristan Harris (Google Former Design Ethicist)” 1’11”20 – 1’11”42¹²

E quando Marks Zuckerberg foi questionado pela influência que o facebook exerceu sobre as eleições no Brasil ele respondeu: “É difícil responder. É que...A verdade é que havia muitos fatores em jogo. - Mark Zuckerberg (Facebook Founder)” 1’12 – 1’12”06.

As empresas de telefonia e de saneamento têm dados importantes sobre as pessoas, senão vejamos:

As empresas de telefonia tem dados importantes sobre você, por isso temos leis que garantem que não sejam mal utilizados. Não temos

¹⁰ O DILEMA das Redes. Diretor Jeff Orlowski /produtora Larissa Rhodes. **Netflix**, 2020. Edward Tufte (Emeritus Professor of Statistics, Graphic Design, and Political Economy at Yale University) 30’49 – 30’55”.

¹¹ O DILEMA das Redes. Diretor Jeff Orlowski /produtora Larissa Rhodes. **Netflix**, 2020. Tristan Harris (Google Former Design Ethicist)” 1’08”27 – 1’08”54.

¹² O DILEMA das Redes. Diretor Jeff Orlowski /produtora Larissa Rhodes. **Netflix**, 2020. Tristan Harris (Google Former Design Ethicist)” 1’11”20 – 1’11”42.

praticamente nenhuma lei que regule a privacidade digital. - Roger McNamee (Facebook Early Venture)" 1'23"22 – 1'23"33¹³

O Roger McNamee, um dos principais investidores do facebook, também se manifestou sobre a influência que as redes sociais têm sobre os seus usuários.

A lei é omissa a respeito disso, mas a situação atual existe não para proteção dos usuários, e sim porque se protege os direitos e privilégios dessas empresas gigantes e incrivelmente ricas. Sempre priorizaremos as pessoas mais ricas e poderosas: Ou vamos dizer: Há momentos em que existe um interesse nacional. Mas há momentos em que o interesse das pessoas, dos usuários, é mais importante do que os lucros de uma pessoa que já é bilionária. - Roger McNamee (Facebook Early Venture)" 1'23"52 – 1'24"20¹⁴

1.2 Proteção de Dados

De acordo com Doneda, “a Privacidade é um direito subjetivo, depende de tempo, classe, condição social, econômica e outros fatores subjetivos.” Doneda também afirma que “A transparência deve ser diretamente proporcional ao poder e a privacidade deve ser inversamente proporcional ao Poder”.

Os dados disponíveis são bens jurídicos muito valiosos, veja o posicionamento de Doneda:

Do ponto de vista quantitativo, os dados disponíveis tornaram - se bem jurídico valiosíssimo, por vezes utilizado escrupulosamente, contendo informações que permitem aos seus detentores conhecerem e traçarem perfis sobre hábitos de consumo, saúde, características genéticas e comportamentais de grande parte da população. ¹⁵

Existem várias formas de identificar um indivíduo, no entanto o nome é o termo utilizado em escala global para identificar a pessoa natural na vida em sociedade,

¹³ O DILEMA das Redes. Diretor Jeff Orlowski/produtora Larissa Rhodes. **Netflix**, 2020. Roger McNamee (Facebook Early Venture)" 1'23"22 – 1'23"33.

¹⁴ O DILEMA das Redes. Diretor Jeff Orlowski/produtora Larissa Rhodes. **Netflix**, 2020. Roger McNamee (Facebook Early Venture)" 1'23"52 – 1'24"20.

¹⁵ DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. São Paulo: Thomson Reuters Brasil, 2019.

mediante registro no órgão competente. A identidade é o conjunto de características pessoais que individualizam o ser humano assim o tornando único, analisamos como o Estado pode conceder a proteção de dados. Na década de 60, surgiram os primeiros grandes projetos de processamento de dados em larga escala e de forma centralizada, esses projetos foram desenvolvidos inicialmente por países considerados de 1º mundo, países desenvolvidos, naquela época havia o início da tutela jurisdicional sobre a segurança jurídica dos dados pessoais.

O foro privilegiado é uma espécie de proteção de dados. No Brasil, temos 45.300 pessoas com foro privilegiado. O objetivo do foro privilegiado é proteger cargos específicos, e não determinadas pessoas. Existe a necessidade de se proteger o exercício da função ou do mandato público.

Os menores de idade, possuem a proteção do pátrio poder para proteger os interesses e estabelecer as obrigações dos pais com seus filhos. Em tempo o poder familiar, segundo Silvio Rodrigues¹⁶, “é o conjunto de direitos e deveres atribuídos aos pais, em relação à pessoa e aos bens dos filhos não emancipados, tendo em vista a proteção destes”. Tomar as decisões e exercer o controle dos dados e das relações jurídicas sob os interesses dos menores sob sua responsabilidade.

Em se tratando aos absolutamente incapazes ou relativamente incapazes, compete a responsabilidade da utilização e proteção dos dados aos responsáveis legais, sejam tutores ou curadores.

Para entrar em conformidade com a nova lei, além dos aspectos jurídicos, existem dois principais pilares tecnológicos que as empresas precisam avaliar internamente para alcançarem o mínimo exigido pela LGPD: governança de dados e segurança da informação. E com a implementação do mínimo exigido, temos as preocupações com relação as pessoas que possuem foro privilegiados, menores de idade, incapazes e pessoas expostas politicamente e relacionados.

¹⁶ RODRIGUES, Silvio. **Direito civil**: direito de família. São Paulo: Saraiva, 2002.

De acordo com o artigo 50, os controladores e operadores “poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização [...] e outros aspectos relacionados ao tratamento de dados pessoais”¹⁷. Esse trabalho de conclusão de curso, sugere boas práticas para exercer tais papéis de controladores e operadores com maior segurança jurídica.

Já o artigo 46 da lei determina que “os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados [...] ou qualquer forma de tratamento inadequado ou ilícito”¹⁸.

É de suma importância que as pessoas físicas tenham conhecimento sobre o quanto os seus dados são valiosos, e que são necessárias várias medidas para evitar a utilização indevida.

O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva”¹⁹.

1.2.1 Da Propriedade do Dado

A norma diz que a propriedade do dado é do titular. E cabe ao titular realizar a gestão dos seus dados. Mas as pessoas não sabem exercer a gestão dos seus dados na totalidade. A lei estabelece uma proteção maior a dados sensíveis, sejam: de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, dados genéticos, biométricos ou sobre a saúde e vida sexual do titular do dado. De todo

¹⁷ BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 10 jul. 2021.

¹⁸ BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 10 jul. 2021.

¹⁹ BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 10 jul. 2021.

modo, só podem ser armazenados sem consentimento os dados indispensáveis para cumprir a lei ou para proteger a vida e a saúde do titular do dado.

Caso ocorra vazamento de dados, os titulares devem ser avisados. As empresas que não atenderem a LGPD, estão sujeitas a falhas de segurança, e podem ser penalizadas com sanções administrativas inclusive multas de até R\$ 50 milhões.

Os órgãos de pesquisa, desde o marco da LGPD sempre que possível devem tornar anônimos os dados pessoais sensíveis. Com relação à proteção dos dados de menores de idade, um dos responsáveis (legais/pais) deve dar consentimento específico ao uso de dados pessoais de crianças e adolescentes.

O titular do dado, ou seja, o “dono da informação pessoal” poderá pedir acesso a qualquer momento a seus dados para corrigir, bloquear ou deletar dados desnecessários. Com relação ao armazenamento de dados, aqueles que estão armazenados fora do Brasil só podem ser compartilhados com países que também possuem legislações que protegem dados.

2 DA REALIDADE NAS EMPRESAS

Quem tem maior acurácia do dado, e a melhor modelagem detém o poder. Ao acessar a internet por exemplo, de qualquer equipamento, navegar em um site, realizar compras online e até um simples fornecimento do CPF em uma loja são etapas de um processo que inicia se com o cadastro, e que quando não possuem políticas e mecanismos de segurança, estão suscetíveis a fraudes e a invasões em banco de dados, utilizações indevidas ou sem consentimento do titular do dado.

Ao realizar a identificação ou a confirmação positiva em um atendimento telefônico também ocorre uma exposição sensível de dados. Esses dados, quando coletados, são utilizados em campanhas publicitárias, campanhas eleitorais, influenciando as pessoas até mesmo com sugestões de compras em sua *timeline*. Existem também pessoas de má fé que utilizam os dados para realizar compras, empréstimos, abertura de contas em instituições bancárias de forma fraudulenta com dados de terceiros. Desta forma essas pessoas de má fé, estão sujeitas a sanções de acordo com o Código Penal.

Existem empresas com *know how* de mercado e que podem realizar o serviço de tratamento dos dados pessoais para outras empresas com segurança. É possível saber se uma empresa está de acordo com a lei geral de proteção de dados. Como uma empresa irá capturar os dados pessoais de seus clientes? Qual é o benefício que as pessoas físicas terão com a LGPD? Quais são os mecanismos de segurança necessários para que as empresas possam realizar o tratamento de dados pessoais de seus clientes e funcionários à luz da LGPD? Todas essas questões serão respondidas neste trabalho.

Com relação a responsabilidade civil das empresas, na LGPD está positivada, e tais dispositivos não serão aplicáveis em todos os casos envolvendo responsabilidade civil, podendo ocorrer culminação de sanções, como o Código e Defesa do Consumidor. Tal responsabilidade não limita -se a existência do dano,

normas que caso não sejam seguidas, haverá sanções. É preciso mudar a cultura para interiorizar a LGPD.

Foi possível observar que todas as empresas que participaram da pesquisa, necessitarão de modificações nos seus processos internos de armazenamento de dados, além de alterações na segurança da informação. Os escassos recursos tecnológicos são um limitador para adequação à lei, assim como o desconhecimento das melhores práticas em segurança da informação. Nesse sentido, recomenda-se que as seguintes mudanças sejam aplicadas como passos iniciais para adequação à LGPD:

- criação de uma política de segurança da informação conforme a regra de negócio da organização;
- plano de formação com treinamento para os funcionários;
- definição do responsável pelo tratamento de dados; mudanças no sistema de gestão empresarial (Enterprise Resource Planning ou ERP) para adequação aos direitos dos titulares dos dados;
- utilização de consultorias externas para auxiliar a organização na adequação à LGPD.
- implementar um plano de comunicação interno sobre os benefícios, deveres e responsabilidades de cada funcionário a luz da LGPD.

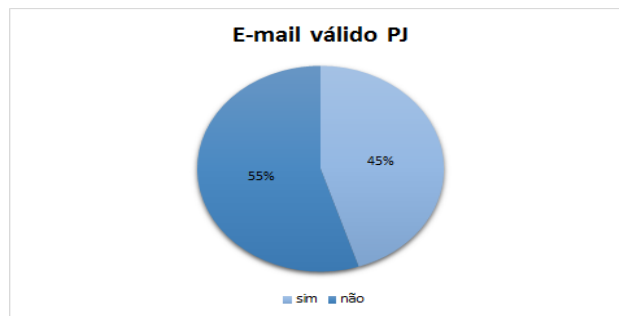
Dentre as obrigatoriedades estabelecidas pela LGPD, o tema associado ao desligamento/demissão de funcionários e a portabilidade dos dados pessoais foi o mais polêmico e acreditamos que ainda será bastante discutido.

O Brasil deu um passo importante para a proteção e privacidade dos dados pessoais, adequando-se às práticas de países desenvolvidos. E por ser um país de tamanho continental, pode apresentar consideráveis discrepâncias nos estudos realizados em diferentes regiões do país, podendo ser uma abordagem interessante em novos estudos. Mesmo sendo utilizado princípios metodológicos essenciais a um

trabalho dessa natureza, limitações podem ser consideradas. A responsabilidade civil decorre de uma conduta voluntária de um dever jurídico.

Do público que respondeu a pesquisa, 55% responderam com e-mail da empresa válido, ou seja, tiveram segurança de fornecer o e-mail correto. Os demais 45 % dos respondentes, não responderam com e-mail válido.

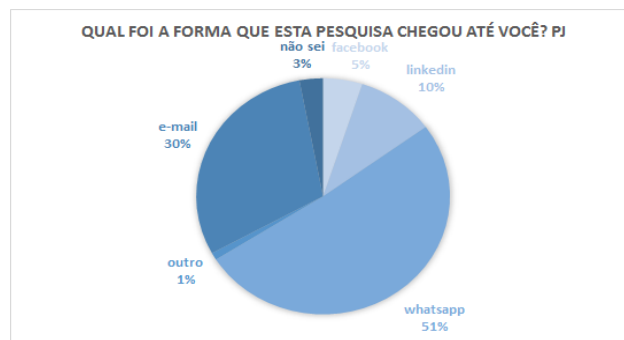
Figura 1 – E-mail válido pesquisa PJ



Fonte: Elaboração própria.

Um das perguntas realizadas foi sobre como a pesquisa chegou até aquela empresa, e 51% das empresas receberam a pesquisa via whatsapp, 30% receberam a pesquisa por e-mail, 10% receberam via linkedin, 5% receberam a pesquisa via facebook, 3% não lembra e 1% outro meio.

Figura 2 – Como a pesquisa chegou até a empresa pesquisa PJ

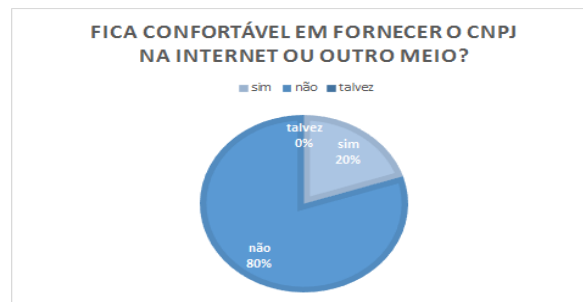


Fonte: Elaboração própria.

Foi perguntado se o responsável da empresa estava confortável em fornecer o Cadastro Nacional de Pessoa Jurídica (CNPJ) na internet ou em outro meio, seja para realizar consultas, pesquisas, até em responder essa pesquisa. E recebemos a resposta de que 80% das empresas respondentes não se sentiam confortáveis em

fornecer o CNPJ na internet ou por outro meio e 20% sentiam se confortáveis em fornecer essa informação.

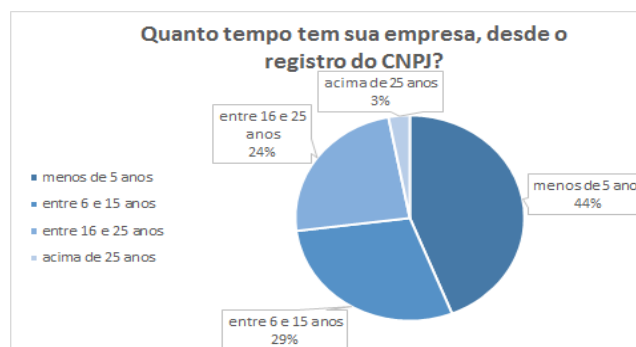
Figura 3 – Fica confortável em fornecer o CNPJ na internet ou outro meio



Fonte: Elaboração própria.

Na pesquisa também foi questionado quanto tempo tem a empresa, desde o registro do CNPJ. E considerando o lapso temporal da pesquisa que ocorreu durante um dos picos da pandemia COVID no Brasil, tivemos o retorno de que 44% das empresas tinham menos de 5 anos de registro, 29% tinham entre 6 e 15 anos de registro, 24% tinham entre 16 e 25 anos e 5% acima de 25 anos de registro.

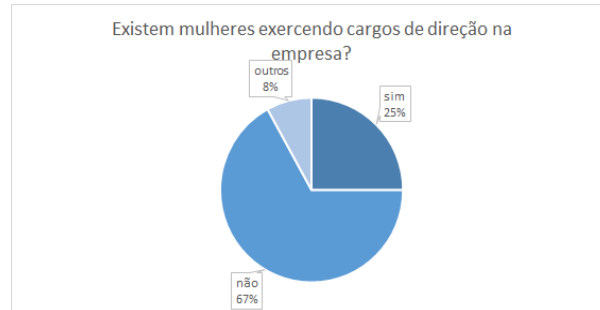
Figura 4 – Tempo de empresa desde o registro do CNPJ



Fonte: Elaboração própria.

Foi questionado se existem mulheres exercendo cargos de direção na empresa. E dentre as empresas respondentes 67% informaram que não tem mulheres exercendo cargos de direção na empresa, 25% responderam que sim tem mulheres exercendo cargos de direção na empresa e 8% responderam outros.

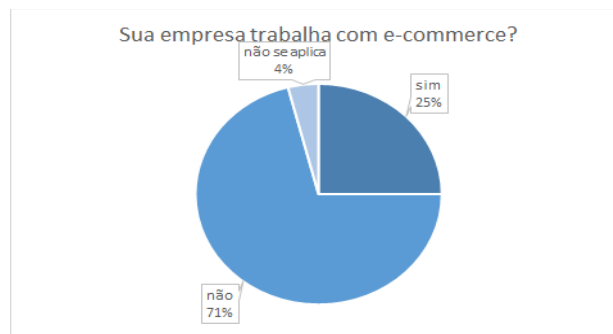
Figura 5 – Existem mulheres exercendo cargos de direção pesquisa PJ



Fonte: Elaboração própria.

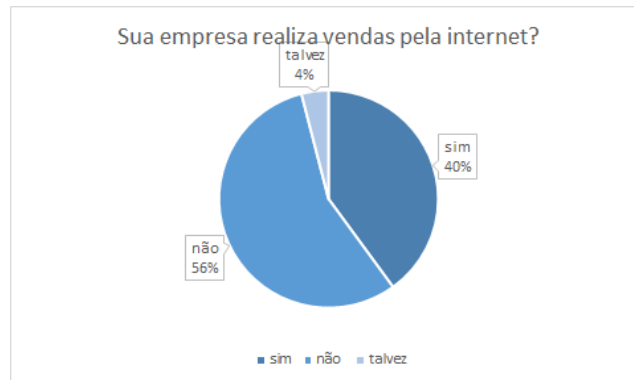
Uma das perguntas da pesquisa foi se a empresa trabalha com e-commerce. Em português, a expressão significa todo tipo de comercialização através da internet. Dentre os respondentes, 71% informaram que não trabalham com e-commerce, 25% disseram que sim trabalham e 4% informaram que o ramo da empresa não se aplica ao e-commerce.

Figura 6 – Trabalha com e-commerce PJ



Fonte: Elaboração própria.

Em outra pergunta, foi questionado se a empresa realiza vendas pela internet. E o retorno consolidado foi diferente. Isso ocorreu pela falta de clareza do empresário sobre o assunto. Sendo que 56% informaram que não trabalham com vendas pela internet, 40% responderam que sim trabalham e 4% responderam que talvez.

Figura 7 – Trabalha com vendas pela internet PJ

Fonte: Elaboração própria.

Foi apresentada uma relação com opções para que o empresário pudesse marcar o dentre as opções, marcar aquela (s) que, segundo o seu entendimento, referem se a DADO PESSOAL. De acordo com a LGPD no art. 5º considera se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável. Diante das respostas consolidadas, identificamos a falta de entendimento da maioria dos entrevistados sobre o que é o DADO PESSOAL. Todas as empresas informaram que nome, dados biométricos para identificar o humano, informações relacionadas a saúde e sobre a vida sexual ou orientação sexual são dados pessoais. Nenhuma empresa informou que informações sobre filiação sindical e dados genéricos são dados pessoais.

Tabela 1 – Consolidado Dado Pessoal pesquisa PJ

Nome	100
dados biométricos para identificar o ser humano	100
relacionados a saúde	100
a vida sexual ou orientação sexual	100
eletrônica (e-mail, endereço de IP)	98
número de identificação	92
identificador de publicidade do telefone	90
dados de localização	80
Morada	76
testemunhos de conexões (cookies)	61
convicções religiosas ou filosóficas	50
opiniões políticas	39
origem racial ou étnica	12
filiação sindical	0
dados genéricos	0

Fonte: Elaboração própria.

Foi dada uma relação com opções para que o empresário pudesse marcar o dentre as opções, marcar aquela (s) que, segundo o seu entendimento, referem se a DADO PESSOAL SENSÍVEL. Diante disto, tivemos o retorno abaixo. De acordo com a LGPD Art. 5º Para os fins desta Lei, considera-se [...] II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Considerando as respostas consolidadas dos empresários, é nítido a falta de clareza sobre a diferença entre os detalhes da legislação vigente. Dentre os respondentes, todos disseram que dados de localização são dados sensíveis. Nenhum respondente afirmou que dados genéricos ou de filiação sindical fossem sensíveis.

Tabela 2 – Consolidado Dado Pessoal Sensível pesquisa PJ

dados de localização	100
a vida sexual ou orientação sexual	99
eletrônica (e-mail, endereço de IP)	98
relacionados a saúde	98
Morada	94
dados biométricos para identificar o ser humano	92
número de identificação	90
opiniões políticas	85
convicções religiosas ou filosóficas	85
testemunhos de conexões (cookies)	83
origem racial ou étnica	69
identificador de publicidade do telefone	34
Nome	24
filiação sindical	0
dados genéricos	0

Fonte: Elaboração própria.

Em uma das perguntas da pesquisa, foi questionado dentre os setores abaixo, selecione aquele que sua empresa se enquadra. É válido mencionar que essa é a visão consolidada de que os empresários participantes têm sobre o setor do negócio.

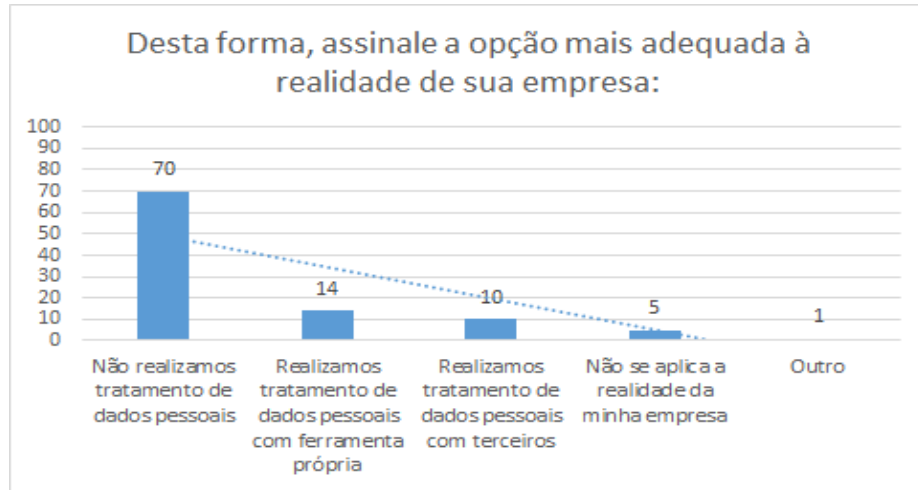
Tabela 3 – Setores que participaram da pesquisa PJ

prestação de serviços	31
Varejo	25
alimentos	10
escritórios de advocacia	7
logística	6
engenharia	6
farmácias	4
hospitais	3
financeiro	3
recursos humanos	2
seguros	2
industria	1

Fonte: Elaboração própria.

A LGPD define em seu art. 5º, inc. X o TRATAMENTO como “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” executadas mediante emprego de ferramentas tecnológicas, seja identificando padrões de comportamento humano, catalogando-as, classificando-as ou etiquetando indivíduos. Diante desta afirmação, na pesquisa foi solicitado que o empresário escolhesse a opção mais adequada à realidade. E de acordo com o retorno, 70% responderam que não realizam tratamento de dados pessoais, 14% realizam tratamento de dados pessoais com ferramenta própria, 10% realizam tratamento com terceiros, 5% não se aplica a realidade da empresa no que tange a tratamento e 1% respondeu outros.

Figura 8 – Empresas que realizam tratamento de dados



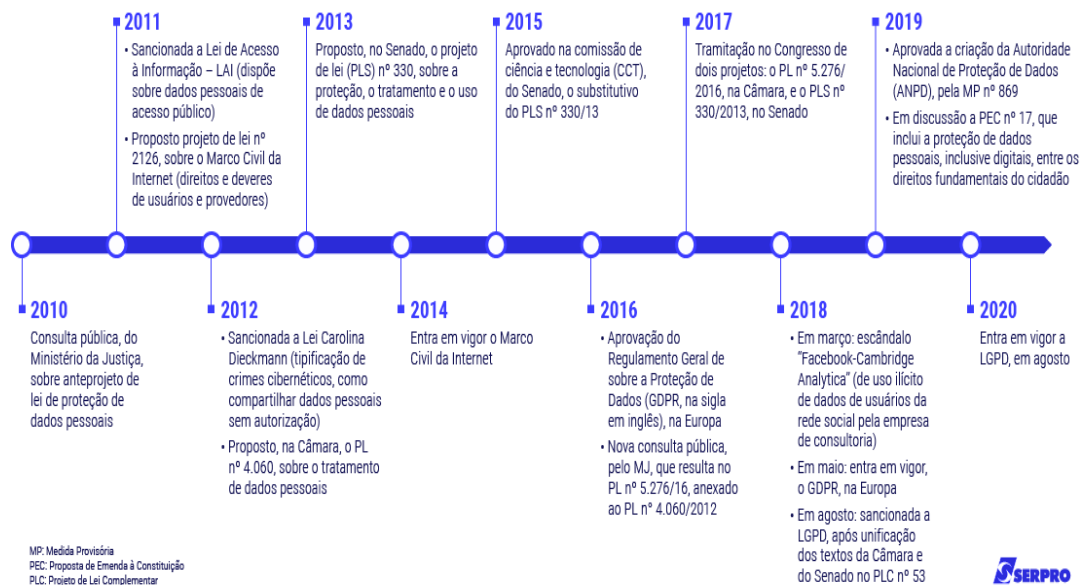
Fonte: Elaboração própria.

Considerando o retorno da pesquisa realizada com as empresas, identificamos que a maior parte não está de acordo com as premissas da LGPD. Muitos não responderam sobre como a empresa realiza a captura de dados, e sobre esse fluxo e a segurança deste processo de captura de dados na empresa.

3 DA LEGISLAÇÃO VIGENTE

Logo abaixo é possível visualizar uma linha do tempo da proteção de dados pessoais e da Lei Geral de Proteção de Dados Pessoais, no Brasil. Hoje no mundo, mais de 109 países possuem leis gerais de proteção de dados pessoais vigentes.

Figura 9 – Linha do Tempo proteção de dados pessoais e LGPD Serpro



fonte: [Linha do tempo da proteção de dados pessoais e da Lei Geral de Proteção de Dados Pessoais, no Brasil — LGPD - Lei Geral de Proteção de Dados Pessoais | Serpro](#)

A Alemanha na década de 70 estruturou a primeira legislação no Estado de Hesse sobre a proteção de dados. A implementação desta lei estadual estruturou a criação de uma lei federal posteriormente. Na mesma década, olhando para o Brasil, tivemos o início do cadastro e controle de dados pelo governo federal. Até aquele momento, não existia transparência, segurança e estrutura tecnológica para a gestão de dados.

3.1 União Européia

Em 1995, houve a *Data Protection Directive* (Europa). Naquele momento, era uma regulamentação sobre o processamento de dados pessoais na Europa. No cenário mundial, existe um debate sobre a Proteção de Dados, concomitante à Regulação Geral de Proteção de Dados (GDPR, na sigla em inglês).²⁰

A norma na Europa foi aprovada em 2016, atualizando o regulamento de 1995. Tal norma tem impactos não apenas na Europa, mas é usada como referência nas relações comerciais de países europeus com outros países, inclusive o Brasil. O regulamento Europeu é aplicável desde 25 de maio de 2018 em todos os Estados membros para harmonizar as leis de privacidade de dados em toda a Europa.

A GDPR se aplica a qualquer tratamento de dados de pessoas residentes na União Européia, mesmo no caso de empresas sediadas em outros países. Isso inclui firmas que oferecem bens e serviços na região ou monitoram o comportamento de seus cidadãos. Para realização do tratamento dos dados, é necessário obter consentimento do titular, em um pedido que deve ser apresentado de forma clara e acessível, garantindo também o direito ao usuário de revogá-lo.

A legislação estabelece uma série de direitos aos cidadãos: acessar as informações que uma empresa tenha, corrigi-las e negar que elas sejam objeto de tratamento.

A lei da União Europeia incluiu um item polêmico, denominado “direito ao esquecimento”, isto é a possibilidade de o usuário solicitar a retirada de suas informações de uma plataforma (como o Google), devendo a empresa avaliar se o pleito não fere o interesse público. A norma também previu o direito de as pessoas não submeter suas informações a decisões automatizadas, como as linhas do tempo do Facebook ou a recomendação de vídeos do YouTube. No Brasil a norma LGPD

²⁰ UNIÃO EUROPÉIA. **Dispõe sobre Proteção de Dados, concomitante à Regulação Geral de Proteção de Dados.** 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/pt/TXT/?qid=1559291025147&uri=CELEX:32016R0679#d1e40-1-1>. Acesso em: 09 set. 2021.

não contempla o direito ao esquecimento. Os ministros do Supremo Tribunal Federal entenderam que o direito ao esquecimento é incompatível com a Constituição Federal brasileira. Apenas o Ministro Edson Fachin entendeu pela compatibilidade do instituto com o texto constitucional e, em razão disso, seu voto foi vencido.

Na Europa, as empresas precisam notificar usuários em caso de um vazamento que implique risco, devem informar se há dados sendo processados assim como e para qual finalidade. E caso instadas ficam obrigadas a fornecer os dados do usuário em um formato que outras máquinas podem ler, instituindo uma espécie de “portabilidade de dados”. As empresas têm de adotar medidas para garantir a proteção dos dados dos usuários. A regulação estabelece penalidades como multas de até 20 milhões de euros ou de até 4% do faturamento anual da empresa punida (o que for maior). Isso vale tanto para quem processa os dados quanto para quem controla, incluindo armazenamentos na “nuvem”.

3.2 Estados Unidos da América

Já os E.U.A. são referência mundial, por lá a legislação é fragmentada. A Lei de Privacidade de Comunicação Eletrônica (ECPA, na sigla em inglês), de 1986²¹, proíbe a interceptação de mensagens telefônicas ou eletrônicas e garante a segurança de informações tanto durante a transmissão quanto no armazenamento, inclusive em computadores.

A norma estabelece também mecanismos distintos de acesso a determinadas informações, separando o que pode ser obtido pelos provedores e o que depende de ordem judicial ou de mandado de busca. Ao longo dos anos, a legislação foi sendo

²¹ ESTADOS UNIDOS DA AMÉRICA. **Lei ECPA. 1986**. Dispõe sobre a Privacidade de Comunicação eletrônica. Disponível em: <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#electronic-communications-privacy-act-of-1986-ecpa-18-u-s-c-%C2%A7%C2%A7-2>. Acesso em: 10 set. 2021.

atualizada para abranger também comunicações digitais. A Lei de Proteção da Privacidade de Crianças (COPPA, na sigla em inglês)²² institui regras para responsáveis por websites e serviços online visando a promoção da privacidade de crianças e adolescentes de até 13 anos na internet. Entre as obrigações estabelecidas pela norma está a de disponibilizar de forma clara sua política de privacidade para este público.

A coleta de informações de meninos e meninas, salvo exceções, fica condicionada à obtenção de consentimento dos pais que também podem corrigir ou solicitar a exclusão dos registros. Pela regra, websites e serviços online ficam proibidos de repassar informações coletadas de crianças a terceiros, devendo mantê-las somente enquanto forem necessárias no processo de tratamento.

Há também normas setoriais, como a Lei de Portabilidade e Transparência de Seguros de Saúde (HIPAA, na sigla em inglês), de 1996. A regulação trouxe obrigações como notificar órgãos públicos (secretarias de saúde) e até veículos de imprensa em caso de vazamentos. Também estabelece padrões de segurança para os dados médicos, a proibição do uso ou repasse de dados a não ser se houver consentimento e salvo em exceções como nas atividades da operadora (como plano de saúde) ou em pesquisas médicas.

A Lei de Privacidade (Privacy Act) fixa as diretrizes para a coleta, armazenamento, uso e disseminação de dados por agências federais. Segundo a norma, esses órgãos precisam divulgar a existência de registros públicos de informações. A disponibilização de dados de indivíduos por essas instituições é condicionada ao consentimento por escrito, a não ser em 12 tipos de situações excepcionais, como a necessidade de uso por um servidor para o exercício de seu

²² ESTADOS UNIDOS DA AMÉRICA. **Lei ECPA**. 1986. Dispõe sobre a Privacidade de Comunicação eletrônica. Disponível em: <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#electronic-communications-privacy-act-of-1986-ecpa-18-u-s-c-%C2%A7%C2%A7-2>. Acesso em: 10 set. 2021.

dever, para fins estatísticos sem a identificação da pessoa, em caso de solicitação do Congresso e por ordem judicial.

Em 2013 houve o escândalo de espionagem em massa pelo governo dos Estados Unidos da América²³. Os jornais “Guardian” e “Washington Post” publicaram primeiro os dados vazados. A reportagem do jornal britânico foi assinada por Glen Greenwald. O caso veio a público após Edward Snowden, ex-técnico da CIA, se apresentar ao mundo e contar que sentiu a obrigação de denunciar ao mundo, os poderes da vigilância acumulados pelo governo dos Estados Unidos, estes feitos foram além da espionagem e atingiram vários países, envolvendo diálogos dos presidentes de vários países inclusive do Brasil.

3.3 América Latina

Na América Latina, diversos países já têm legislações de proteção de dados como Chile, Argentina, Uruguai e Colômbia. A lei chilena, de 1999²⁴, limita o uso dos dados ao propósito informado no ato da coleta, com a exceção de registros tornados públicos. Desta forma, garante aos titulares o direito a acessar as informações de posse de alguma empresa, corrigi-la ou eliminá-la se o armazenamento não respeitar as exigências da Lei ou o tratamento for concluído. A lei prevê a responsabilização de empresas controladoras de dados em caso de prejuízos aos titulares, com sanções definidas pela Justiça. O texto estabelece algumas diferenças para o Poder Público, limitando o tratamento de dados ao previsto na lei e impedindo divulgação de informações sobre condenações depois de prescreverem.

²³ GREENWALD, Glenn; MACASKILL, Ewen; POITRAS, Laura. Edward Snowden: the whistleblower behind the NSA surveillance revelations. **The Guardian**, 11 jun. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Acesso em: 09 set. 2021.

²⁴ CHILE. **Lei nº 19.628 desde 1999**. Dispõe sobre Proteção de Dados. Disponível em: <https://www.bcn.cl/leychile/navegar?idNorma=141599>. Acesso em: 09 set. 2021.

Na Argentina, a Lei de Proteção de Dados Pessoais foi aprovada em 2000²⁵. Ela regula bases de dados públicas e privadas, estabelecendo como princípio o uso limitado à finalidade para a qual foram obtidas. O tratamento está condicionado ao consentimento do titular, que deve ser livre, expresso e informado. Essa autorização não é exigida nos casos de bases públicas, no cumprimento de uma obrigação legal, no exercício de funções próprias do Estado e quando as informações se limitam a nome, identidade, profissão, data de nascimento e endereço.

As empresas são obrigadas a atualizar dados incompletos e errados. Não podem manter registros após o término da atividade para a qual foram coletados. Os entes responsáveis pelo tratamento também devem garantir o acesso dos titulares às suas informações. Mas é permitido o repasse de dados a terceiros desde que cumpram um “interesse legítimo” do ente que os estão cedendo. Já órgãos públicos têm regras especiais, como o direito de negar o acesso, a correção e a supressão das informações. Também há menos obrigações no caso de segurança nacional ou segurança pública.

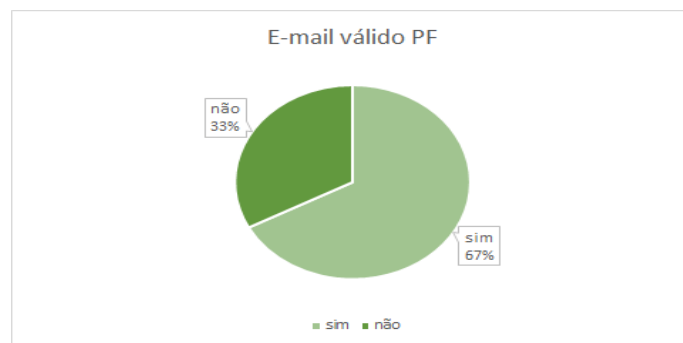
²⁵ ARGENTINA. **Lei nº 25.326 desde 2000**. Dispõe sobre Proteção de Dados Pessoais. Disponível em: http://www.jus.gob.ar/media/3201023/personal_data_protection_act25326.pdf. Acesso em: 01 jun. 2021.

4 POLÍTICAS PÚBLICAS

No Brasil existem normas fragmentadas sobre o assunto. E que para o brasileiro, ainda é vago a ideia de posse e de “dono do dado”. Vejamos os resultados da pesquisa realizada com pessoas físicas:

Dentre o público participante, total de 1.130 pessoas, ao ser pedido um e-mail válido aos respondentes, 67% responderam com a informação válida e 33% não responderam com e-mail válido.

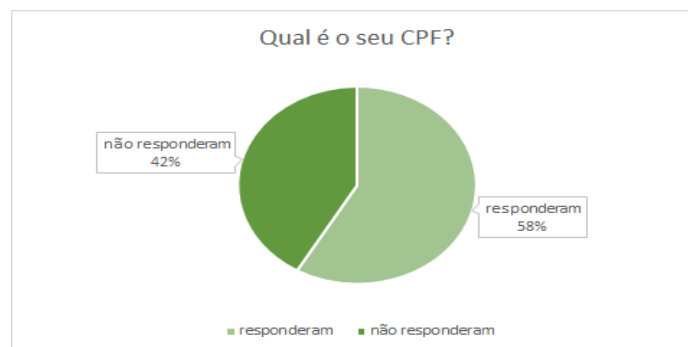
Figura 10 – E-mail válido pesquisa PF



Fonte: Elaboração própria.

Em uma das perguntas realizadas na pesquisa, foi solicitado o número do CPF do participante. Os dados consolidados refletem que 58% responderam o número de CPF conforme solicitado e 42% não responderam com o número de CPF.

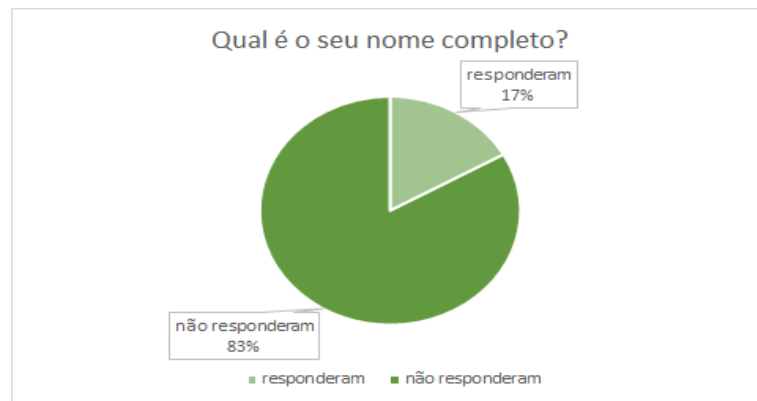
Figura 11 – Forneceram CPF



Fonte: Elaboração própria.

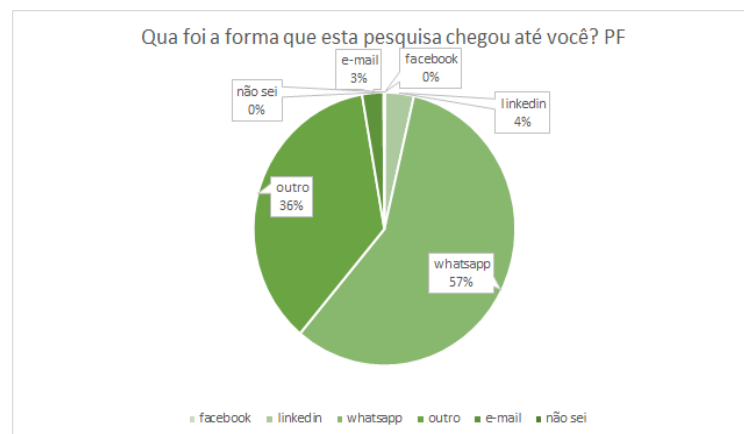
Em uma das perguntas foi solicitado o nome completo do entrevistado. Dentre os respondentes, apenas 17% dos entrevistados responderam o nome completo e 83% não responderam com o nome completo.

Figura 12 – Forneceram nome completo



Uma das perguntas foi sobre como a pesquisa chegou até aquela pessoa, e a resposta consolidada mostra que 57% das pessoas receberam a pesquisa via whatsapp, 36% por outro meio, 4% receberam pelo linkedin, 3% receberam a pesquisa por e-mail.

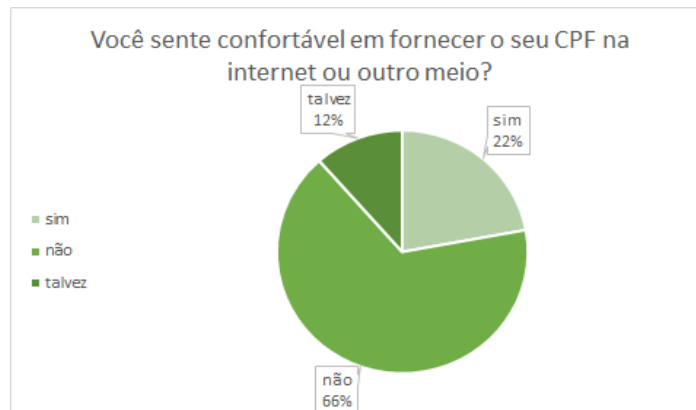
Figura 13 – Como a pesquisa chegou até você pesquisa PF



Foi perguntado se a pessoa se sentia confortável em fornecer o CPF na internet ou em outro meio, seja para realizar consultas, pesquisas, até em responder essa pesquisa. E recebemos a resposta consolidada de que 66% dos respondentes não se sentiam confortáveis em fornecer o CPF na internet ou por outro meio, 22%

estavam confortáveis em fornecer o CPF e 12% dependendo da situação poderiam responder com o CPF ou não. Essa informação reflete o receio que as pessoas têm em fornecer o CPF pela internet ou outro meio quando solicitado.

Figura 14 – Fica confortável em fornecer o CPF na internet ou outro meio



Fonte: Elaboração própria.

Em uma das perguntas foi questionado em qual Unidade Federativa a pessoa reside. De acordo com as respostas consolidadas a pesquisa alcançou todas as Unidades Federativas do Brasil, distribuídos da seguinte forma:

Tabela 4 – Unidade Federativa dos participantes pesquisa PF

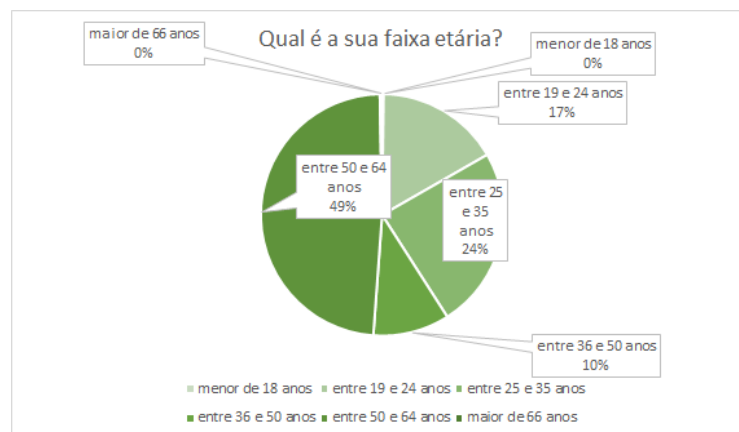
DF	740
GO	40
BA	37
MT	30
RO	30
MG	30
RJ	30
ES	22
AC	20
RO	20
PA	13
SP	13
RN	12

MS	10
AM	10
PA	10
MA	10
PE	10
AL	10
AM	9
TO	6
SC	5
CE	4
SE	4
PR	3
PI	1
RS	1

Fonte: Elaboração própria.

Dentre as perguntas da pesquisa, foi questionado qual é a sua faixa etária. Do total do público respondente, 49% possuem idade entre 50 e 64 anos, 24% possuem idade entre 25 e 35 anos, 17% possuem idade entre 19 e 24 anos, 10% possuem idade entre 36 e 50 anos não houveram respondentes maiores de 66 anos e menores de 18 anos.

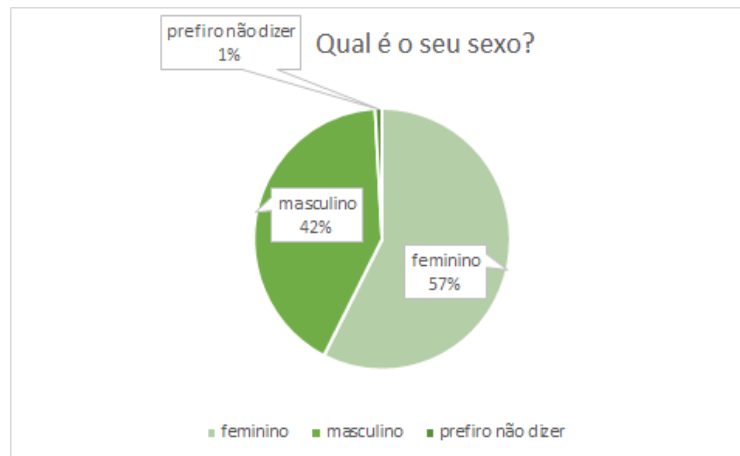
Figura 15 – Distribuição por faixa etária entre os participantes pesquisa PF



Fonte: Elaboração própria.

Em uma das perguntas, foi questionado qual é o sexo da pessoa. Do público respondente, 57% do público entrevistado se identificou como sexo feminino, 42% com sexo masculino e 1% preferiu não dizer.

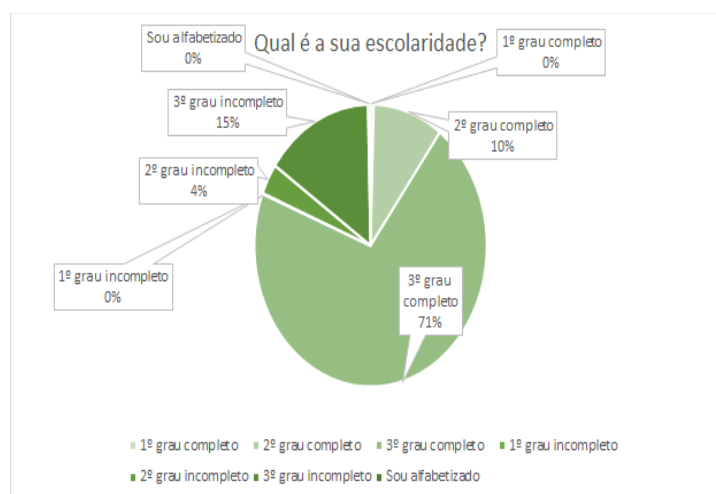
Figura 16 – Distribuição por sexo entre os participantes pesquisa PF



Fonte: Elaboração própria.

Foi perguntado qual é a escolaridade da pessoa. Do público entrevistado, 71% declararam que possuem o 3º grau completo ao serem perguntados sobre a escolaridade, 10% responderam possuir 2º grau completo, 15% responderam que tem o 3º grau incompleto e 4% responderam possuir 2º grau incompleto.

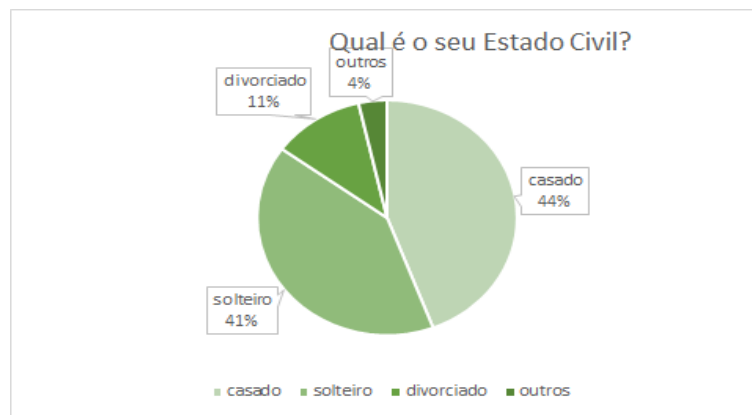
Figura 17 – Distribuição escolaridade dos participantes pesquisa PF



Fonte: Elaboração própria.

Durante a pesquisa, foi questionado qual é o Estado Civil da pessoa. Dentre o público respondente, 44% responderam ser casado, 41% solteiro, 11% divorciado e 4% do público respondente não se pronunciaram sobre esse questionamento.

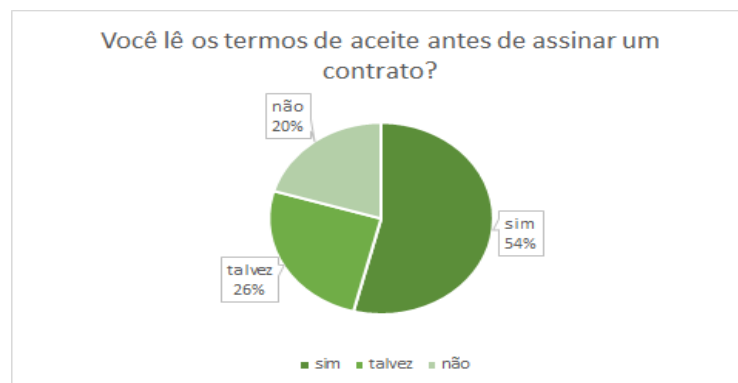
Figura 18 – Distribuição por estado civil entre os participantes pesquisa PF



Fonte: Elaboração própria.

Em determinado momento, foi questionado se o público lê os termos de aceite antes de assinar um contrato. E 54% dos entrevistados disseram que sim leem os termos de aceite antes de assinar um contrato, 26% responderam que não leem e assinam assim mesmo e 26% responderam que talvez, depende da situação ler antes de assinar um contrato. A resposta consolidada é preocupante, tendo em vista que o brasileiro em sua grande maioria não tem o hábito de ler antes de assinar um contrato.

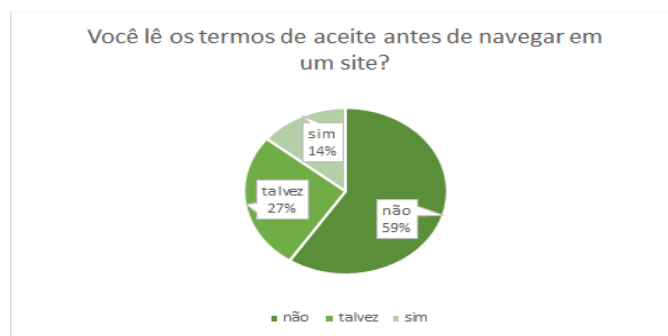
Figura 19 – Distribuição leitura termos de aceite antes de assinar um contrato



Fonte: Elaboração própria.

Dentre as perguntas, o público foi questionado se lê os termos de aceite antes de navegar em um site. E 59% dos entrevistados disseram que não leem o termo de aceite antes de navegar em um site, 14% responderam que sim leem e 27% responderam que talvez, dependendo de cada caso. A resposta consolidada é preocupante, tendo em vista que o brasileiro em sua grande maioria não tem o hábito de ler os termos de aceite antes de navegar em um site.

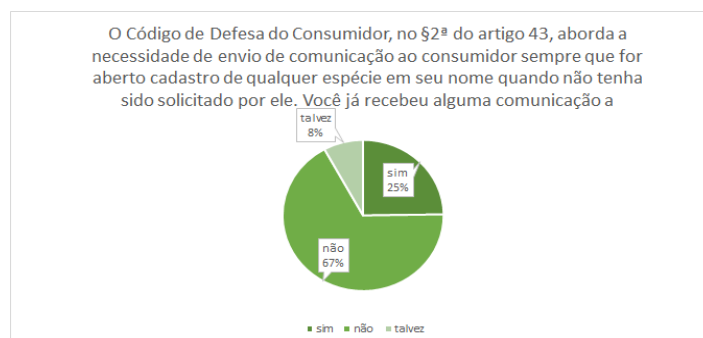
Figura 20 – Distribuição leitura termos de aceite antes de navegar e um site



Fonte: Elaboração própria.

Foi apresentada a seguinte afirmação para o público entrevistado: “O Código de Defesa do Consumidor, no §2ª do artigo 43, aborda a necessidade de envio de comunicação ao consumidor sempre que for aberto cadastro de qualquer espécie em seu nome quando não tenha sido solicitado por ele.” Desta forma foi perguntado se já receberam alguma comunicação a respeito disto. A resposta consolidada foi que 67% nunca recebeu qualquer tipo de informação nestes termos, 25% sim já receberam informações neste sentido e 8% talvez, não lembram. Esse dado demonstra que as empresas não estão cumprindo uma premissa básica da legislação já vigente no país.

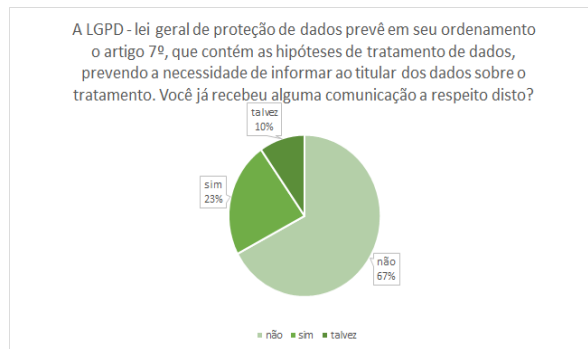
Figura 21 – Publico que já recebeu alguma comunicação conforme CDC



Fonte: Elaboração própria.

Foi apresentada a seguinte afirmação para o público entrevistado: “A LGPD - lei geral de proteção de dados prevê em seu ordenamento o artigo 7º, que contém as hipóteses de tratamento de dados, prevendo a necessidade de informar ao titular dos dados sobre o tratamento.” Desta forma, foi perguntado se já recebeu alguma comunicação a respeito disto. A resposta consolidada foi que 67% não recebeu comunicação, 23% sim receberam e 10% disseram que talvez tenha recebido essa comunicação. Esse dado também é preocupante, tendo em vista que a LGPD está vigente.

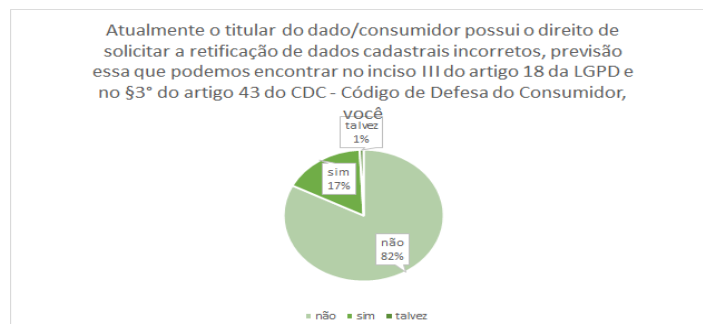
Figura 22 – Publico que já recebeu alguma comunicação conforme LGPD



Fonte: Elaboração própria.

Foi apresentado a seguinte afirmação para o público entrevistado: “Atualmente o titular do dado/consumidor possui o direito de solicitar a retificação de dados cadastrais incorretos, previsão essa que podemos encontrar no inciso III do artigo 18 da LGPD e no §3º do artigo 43 do CDC - Código de Defesa do Consumidor, neste contexto foram questionados se já realizaram algum pedido de alteração de seus dados. A resposta consolidada foi que 82% não solicitaram retificação de dados conforme previsão legal, 17% sim já solicitaram alteração nos dados incorretos e 1% talvez.

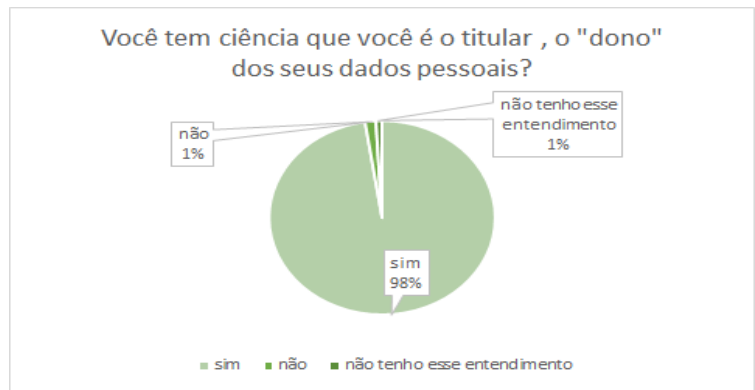
Figura 23 – Publico que já solicitou retificação de dados incorretos conforme LGPD



Fonte: Elaboração própria.

Foi perguntado ao público se a pessoa tem ciência que ele é o titular, o "dono" dos seus dados pessoais. Diante dos resultados consolidados, 98% das pessoas responderam que sim, tem ciência de que é o titular do seu dado pessoal, 1% respondeu que não tem esse entendimento e 1% respondeu que não tinha ciência.

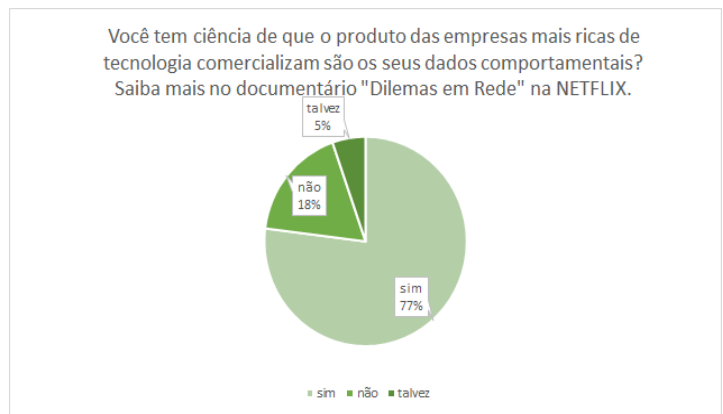
Figura 24 – Distribuição Público que tem ciência de ser o “dono” do dado



Fonte: Elaboração própria.

Foi perguntando se o entrevistado tem ciência de que o produto das empresas mais ricas de tecnologia comercializa são os seus dados comportamentais. Saiba mais no documentário "Dilemas em Rede" na NETFLIX. O resultado consolidado nos apresenta a informação de que 77% tem ciência de que as empresas mais ricas de tecnologia comercializam os dados pessoais e comportamentais, 18% disseram que não tem ciência de que as empresas mais ricas de tecnologia comercializam os dados, 5% respondeu que não tinham tanta certeza.

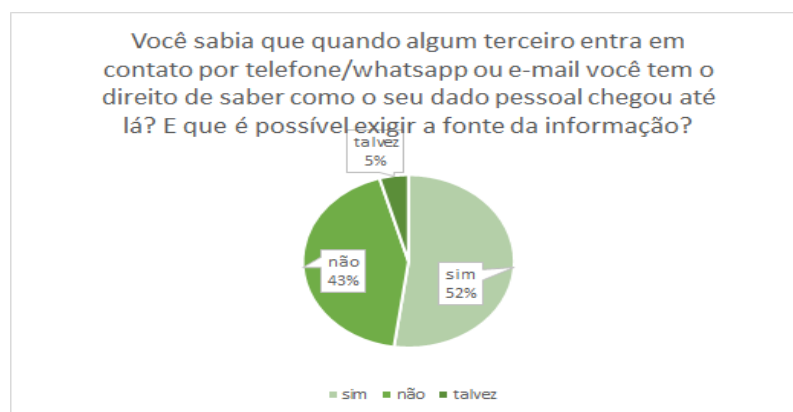
Figura 25 – Público ciente sobre comercialização dos dados comportamentais



Fonte: Elaboração própria.

Foi questionado se as pessoas sabiam que quando algum terceiro entra em contato por telefone/whatsapp ou e-mail ele, como titular do dado, tem o direito de saber como o seu dado pessoal chegou até lá? E que é possível exigir a fonte da informação? A resposta consolidada diz que 52% sim sabiam desta informação e 43% não sabiam disso e 5% não foram específicos.

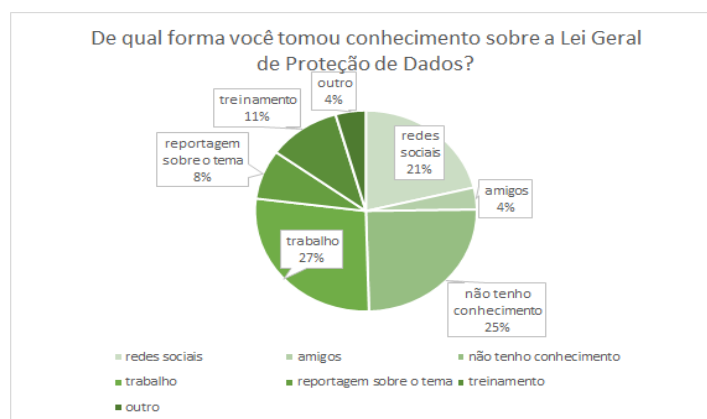
Figura 26 – Público ciente sobre exigir a fonte da informação



Fonte: Elaboração própria.

Foi questionado para as pessoas qual forma tomou conhecimento sobre a Lei Geral de Proteção de Dados. A partir da consolidação das respostas, identificamos que 27% tomaram conhecimento no trabalho, 25% informou que não tem conhecimento sobre a LGPD, 21% responderam que tomaram conhecimento pelas redes sociais, 11% informaram que receberam informações através de treinamento, 8% souberam da LGPD por reportagem sobre o tema, 4% por amigos e 4% por outro meio.

Figura 27 – Forma que o público respondente tomou conhecimento da LGPD



Fonte: Elaboração própria.

Quando nos debruçamos em analisar, já identificamos que a norma está fragmentada, temos alguns pontos de suma importância, senão vejamos:

De acordo com a **Constituição Brasileira de 1988**²⁶, em seu artigo 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; XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996)

A Lei Geral de Proteção de Dados incrementa a tutela dos direitos do consumidor prevista no CDC. O regime previsto pela LGPD não exclui aquele definido pelo CDC. A incidência em comum dos arts. 7º do CDC e 64 da LGPD firmam a conclusão de que os direitos dos titulares dos dados previstos nas respectivas normas devem ser cumulados e compatibilizados pelo intérprete.

Já no **Código de Direito do Consumidor**²⁷, temos positivado: Art. 43º O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de

²⁶ BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Disponível em: www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 01 set. 2021.

²⁷ BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Disponível em: www.planalto.gov.br/ccivil_03/LEIS/L8078.htm. Acesso em: 01 set. 2021.

Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

De acordo com o CDC a abertura de cadastro, ficha, registro e dados pessoais deverá ser comunicada por escrito ao consumidor quando não for solicitada por ele. Desta forma, não vejo como é possível ter tantos créditos pré-aprovados, sem o consentimento do titular do dado. O direito existe, está positivado, mas a cultura deverá ser enraizada nas instituições.

Na Lei que estabelece o **Cadastro Positivo - Lei 12.414/2011**²⁸, temos: Art. 3º Os bancos de dados poderão conter informações de adimplimento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei. § 1º Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado.

A Lei do Cadastro Positivo chegou com o objetivo de mudar o mercado de crédito. No Brasil os consumidores sempre foram avaliados pelo histórico negativo, pelo score de crédito estruturado com informações comportamentais de crédito considerando negativas, protestos, ações cíveis, pagamentos em atraso. E a partir da Lei do Cadastro Positivo as informações de hábitos de pagamento em dia começaram a valer uma pontuação maior com relação ao cálculo de risco de crédito. Até mesmo no compartilhamento das informações positivas, o consumidor pode pedir para sair e controlar quem está compartilhando ou não as informações positivas que são essenciais na concessão de crédito hoje.

Já a Lei de Acesso a Informação, positivou alguns conceitos que não faziam parte da norma jurídica e precisavam de legislação para vigorar. Essa norma definiu o que é informação pessoal, a forma de tratamento e reiterou a importância da manutenção do direito a intimidade, vida privada, honra e imagem das pessoas, assim

²⁸ BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Lei do Cadastro Positivo. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 5 set. 2021.

como liberdades e garantias individuais. A norma estruturou a forma de tratamento de dados no Brasil e complementa a LGPD.

Na Lei de **Acesso à Informação - Lei 12.527/2011**²⁹, temos positivado: Art. 4º Para os efeitos desta Lei, considera-se: [...] IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável; [...] Art. 31º O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido. § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico; II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; III - ao cumprimento de ordem judicial; IV - à defesa de direitos humanos; ou V - à proteção do interesse público e geral preponderante. § 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância. § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

Já o **Marco Civil da Internet - LEI 12.965/2014**³⁰, não garante a privacidade e a proteção de dados de forma abrangente, completa e estruturada. O Marco Civil da Internet não é uma normativa geral sobre proteção de dados pessoais.

²⁹ BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Lei de Acesso à Informação. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 10 set 2021.

³⁰ BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 set. 2021.

Regras “clássicas” de proteção de dados pessoais:

- CONSENTIMENTO - Exceções: Dados indispensáveis para a execução de um contrato ou obrigação legal do fornecedor (Art. 7º, VII e IX, e 16, I, do MCI);
 - TRANSPARÊNCIA (Art. 7º, VI, VIII e XI do MCI e 6º,III do CDC).
 - PROTEÇÃO CONTRA A DISCRIMINAÇÃO (Art. 4º, III, e 6º,II, do CDC);
 - COMUNICAÇÃO EM CASO DE VAZAMENTO (Art. 7º, XIII e Art. 10º, §1º do CDC);
 - SEGURANÇA DA INFORMAÇÃO E DOS SISTEMAS (Art. 2º,V, e 10, §4º do MCI);
 - RESPEITO AO CONTEXTO - Utilização de dados deve ser compatível com o contexto em que os dados foram coletados (Art. 7º, VIII do MCI);
- Regras inovadoras de proteção de dados pessoais:
- Controle de práticas abusivas: uso e compartilhamento de dados de forma incompatível com as finalidades do contrato inicial
 - Garantia da confidencialidade da comunicação (independente da natureza do provedor de serviço)
 - Garantia da confidencialidade no armazenamento.

No Brasil existem 4 bureaus de crédito que são associados da ANBC, abordamos todos eles para que pudessem se manifestar sobre a LGPD através de uma entrevista transcrita em formulário com respostas abertas. Recebemos o retorno dos dois maiores birôs de crédito no Brasil: Serasa Experian e BVS/SCPC. Cabe ressaltar que cada bureau realizou um plano de adequação a LGPD e executou o seu papel com relação a segurança de um dos pilares do seu *core business*, o tratamento dos dados.

No site de cada um dos bureaus, é possível ter acesso a um ambiente do consumidor onde o “dono do dado” ou melhor, o titular do dado poderá acessar, realizando um cadastro prévio com validações. No ambiente do consumidor é possível acessar informações pessoais, informações restritivas, score negativo e score

positivo, pedido de alteração cadastral, além de realizar acordos de dívidas ou parcelas em aberto com o comércio e bancos em geral.

Considerando a entrevista com os principais *players* do mercado, realizamos os questionamentos abaixo:

BVS/SCPC

DPO - Data Protection Officer - Viviane Rico Menezes

Gerente Jurídico

Presidente - Dirceu Jodas Gardel Filho

1) Quais foram as adequações realizadas por este bureau de crédito para atender à LGPD?

Resposta. Foram mapeados os riscos referentes a legislação, definição interna de responsabilidades, desenvolvimento de controles de para os casos em que a empresa é controladora e operadora, foram feitas adequações e manutenções nos processos/serviços/produtos, elaboração de novos processos e controles internos de monitoração e adequação e a aplicação de campanhas de treinamento e conscientização de todos os envolvidos.

2) Considerando o know how deste bureau. Quais são as recomendações para a realização do tratamento de dados pessoais de clientes e funcionários?

Resposta. Conhecer as informações, mapear todo o fluxo de tratamento de dados, identificar e tratar as principais vulnerabilidades que possam impactar a empresa, estabelecer políticas de tratamento e adequação de contratos, termos de confidencialidade e responsabilidade, por fim realizar campanha contínua de treinamento e conscientização.

3) No Brasil, quais são os desafios que o bureau encontrou para atender a LGPD?

Resposta. Estabelecer finalidade e bases legais adequadas para todos os dados e produtos fornecidos, estabelecer processos internos para atendimento dos

direitos dos titulares, manter os requisitos de registro de fluxo de tratamento de dados e relatório de impacto atualizados, considerando a constante mudança no ambiente e o grande volume de dados, garantir medidas técnicas de proteção de dados adequadas tanto no ambiente da empresa quanto nos fornecedores e clientes que recebem informações.

4) Na sua opinião, a LGPD possui lacunas? Outras normas vigentes atendem essas lacunas?

Resposta. Há necessidade de estabelecimento de regras de fiscalização, tratamento de dados por pequenas e médias empresas, definição em relação as obrigações de dados governamentais, estabelecimento e aplicabilidade da necessidade de um encarregado de dados, exploração das medidas técnicas adequadas, parâmetros específicos de uso de dados de menores e idosos, definição de prazos razoáveis para atendimento de direitos, exposição de provas etc. Algumas jurisprudências e leis preenchem as lacunas, mas a ANPD ainda tem um longo trajeto para especificar todas as necessidades.

5) Considerando sua experiência no mercado de bureaus de crédito, quais são os prós e contra hoje da LGPD? E a longo prazo, quais são os prós e contras?

Resposta. Vejo muitas vantagens em relação à transparência, definição adequada de tratamento de dados, necessidade regulatória de manter a qualidade dos dados, obrigação em criar um ambiente seguro para manter a proteção da informação entre diversos outros benefícios. Referente às desvantagens, creio que é um período momentâneo de adequação de produtos e serviços, mas quando o tema estiver enraizado no segmento e as empresas estiverem atuando com o 'Privacy by Design e Privacy by Default' na prática, o tema deixará de ser um problema e se tornará mais uma proteção para as empresas do segmento.

6) Deixe sua sugestão/opinião.

Resposta. Estamos vivendo o início do tema LGPD, há ainda um caminho longo de conhecimento e adequação, inclusive globalmente sobre o tema e sem dúvida esta é uma área de conhecimento que será enraizada no mercado. A medida

em que o tempo passa, aumentará a consciência das empresas em relação a necessidade do uso do método de 'Privacy by Design' e 'Privacy by Default', em contrapartida aumentará também a exigência dos titulares de dados. As empresas, especialmente os Bureaus de Crédito, devem iniciar um estudo estratégico de médio e longo prazo para não serem impactadas bruscamente à medida em que as regulamentações de privacidade se expandirem no mercado e os titulares se tornem mais exigentes.

SERASA EXPERIAN

DPO Emiliano Tozetto

Gerente Jurídico Lia Cunha

Presidente Valdemir Bertolo

1) Quais foram as adequações realizadas por este bureau de credito para atender à LGPD?

Resposta: Foram adotadas as medidas necessárias para garantir o cumprimento das normas de proteção de dados pessoais, como, por exemplo: revisão das bases legais aplicáveis aos tratamentos realizados; critérios de observância dos princípios de tratamento; jornadas de atendimento aos titulares para garantia dos seus direitos; transparência sobre o tratamento de dados pela Serasa Experian por meio do Portal de Proteção de Dados Pessoais; revisão e criação de políticas internas específicas para o tratamento de dados pessoais, como a política de retenção e descarte; segregação de bases de dados; treinamento dos funcionários da Companhia; e revisão dos termos de uso e política de cookies.

2) Considerando o know how deste bureau. Quais são as recomendações para a realização do tratamento de dados pessoais de clientes e funcionários?

Resposta: A observância das condições previstas tanto na LGPD quanto em outras legislações que versem, indiretamente, sobre o tratamento de dados, como Código de Defesa do Consumidor, Lei do Habeas Data, Lei do Cadastro Positivo e Marco Civil da Internet. Além disso, a preocupação com a segurança dos dados tratados deve ser prioridade e as empresas precisam ter o compromisso de proteger

a privacidade dos titulares dos dados de forma absolutamente séria. No caso da Serasa Experian, a Companhia possui diversas políticas internas que determinam critérios de segurança da informação e, também, políticas sobre o tratamento de dados que abrangem, dentre outros aspectos, definição de regras gerais para o tratamento de dados pessoais, inclusive quanto às hipóteses de tratamento, princípios, tratamento de categorias especiais e rastreabilidade de todo o ciclo de vida das informações tratadas. Recomenda-se, portanto, tratar as informações conforme legislação vigente, com uma robusta governança das informações, critérios robustos de segurança da informação e fluxos definidos para atendimento aos direitos do titular.

3) No Brasil, quais são os desafios que o bureau encontrou para atender a LGPD?

Resposta: Entendo que o principal desafio foi o caráter genérico da legislação e falta de um órgão operante para consultoria no processo de adequação à LGPD. Especialmente para um bureau, cujo core business é o tratamento de dados, o processo de adequação é longo e custoso e a falta de um órgão regulador operante para eventual esclarecimento acerca da aplicação da lei tornou o processo mais moroso.

4) Na sua opinião, a LGPD possui lacunas? Outras normas vigentes atendem essas lacunas?

Resposta: Sim, possui. Algumas lacunas podem ser parcialmente atendidas por outras normas vigentes mas, considerando a especificidade e recência da LGPD, a maioria das lacunas não é atendida por outras legislações, sendo abertas a interpretações diferentes pelos agentes de tratamento.

5) Considerando sua experiência no mercado de bureaus de crédito, quais são os pros e contra hoje da LGPD? E a longo prazo, quais são os pros e contras?

Resposta: É sabido que o tema é uma preocupação mundial e que, com o avanço da tecnologia, é esperado que as discussões e aplicabilidade de legislações sobre proteção de dados continuem crescendo. Entendo que os principais pontos contra são os elevados custos relacionados à adequação e a ausência atual de apoio

consultivo de órgãos reguladores. Os principais pontos a favor são a própria privacidade e confiança dos titulares e, ainda, o diferencial competitivo ao mercado.

6) Deixe sua sugestão/opinião. Resposta: N/A

CONCLUSÃO

Normas voltadas à proteção de dados pessoais são recentes no Brasil. A estratégia para fortalecer o mercado se deu com as diretrizes trazidas pela lei para processamento de dados pessoais, que geram desafios operacionais e demandam investimento de recursos e tempo. As empresas terão que passar por mudanças relevantes em seus ambientes de TI.

O primeiro passo é iniciar a identificar os dados pessoais, sensíveis, públicos, anonimizados, e de crianças e adolescentes, que a empresa possui em seu banco de dados. Posteriormente, mensurar o nível de exposição da empresa à lei. Além disso, é de suma importância identificar o fluxo de como esses dados são atualizados e o nível de segurança deste processo.

Será necessário a criação de regras, boas práticas e de governança, que determinem normas de segurança e procedimentos de mitigação de riscos no tratamento de dados pessoais.

Um programa LGPD poderá ser estruturado, partindo da premissa de que os processos são contínuos e retroalimentados entre si: Dados, Legal & Compliance, Consumidor, Serviços Compartilhados, REDE/TI, Comunicação e Produtos. E considerando a utilização de um seguro correspondente ao grau do risco de exposição.

Em relação a tratamento de dados, as empresas devem ficar atentas às 20 atividades descritas no artigo 5º, Inciso X, entre elas: coleta, acesso, distribuição, armazenamento e eliminação. Todas elas devem estar aderentes aos princípios gerais descritos no artigo 6 da lei, através da criação e revisão de contratos, termos e políticas para uso interno e externo.

Gestão do consentimento e anonimização, e gestão dos pedidos dos titulares são dois procedimentos importantes perante a LGPD. Investir em controles de solicitações dos titulares e na criação de um banco de dados com todos os pedidos,

são boas estratégias de negócio para que as empresas fortaleçam a confiança com os titulares dos dados.

Em atendimento às exigências da Autoridade Nacional de Proteção de Dados e de outros órgãos do Sistema Nacional de Proteção do Consumidor, é necessário que o controlador disponha do Relatório de Impacto para prestar contas sobre os processos de tratamento de dados. A condução indevida do relatório pode caracterizar-se como uma violação da lei e multas simples ou diárias podem ser aplicadas.

O relatório de Impacto à Proteção de Dados Pessoais deverá ser criado após o controle obrigatório considerando processo organizacional da Segurança da Informação, Identificação da Base Legal, Gestão de Risco de Segurança da Informação e Proteção de Dados Pessoais, Definição do Tempo de Guarda e Identificação da Coleta de Dados Pessoais.

Os requisitos mínimos para o conteúdo do relatório de impacto a Proteção de Dados Pessoais – LGPD conforme art. 38 – parágrafo único, são: Descrição dos Tipos de Dados Coletados, Metodologia utilizada para a coleta, metodologia utilizada para a garantia da segurança das informações e Análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

A LGPD é uma norma efetiva para a proteção de dados pessoais, regulamentando mecanismos de segurança, evitando a invasão dos Banco de Dados e a utilização indevida.

Segue sugestão para implementação de um Governança de LGPD:

- TITULARES: atendimento direto a titulares, gestão de consentimento, gestão de dados de menores e gestão de dados sensíveis.
- CULTURA: treinamento, conscientização e políticas e diretrizes.
- PRIVACIDADE: Contratos e Fornecedores Mapeamento

- **PROTEÇÃO DE DADOS:** Gestão de Acessos, Gestão de Vulnerabilidades (ambiente de TI), Governança de Dados/Ciclo de Vida dos Dados. Anonimização/criptografia e indicadores.

Certamente são irrefutáveis os benefícios para a Pessoa Física sobre a LGPD. Na atualidade, mais do que nunca, a pessoa tem o “poder” da informação, sobre si próprio. A liberdade e privacidade são direitos que transcendem a vida e se reverberam pela eternidade no ambiente digital. E essa exposição on line cria uma reputação que muitas vezes, não foi almejada pelo dono do dado, mas por alguém que iria lucrar mais do que o titular do dado. A pessoa física tem o controle sobre a utilização, atualização e destino dos seus dados.

A invasão dos dados sempre tem um objetivo, demonstrar poder, é a mais pura demonstração de poder quebrar regras e desafiar as normas vigentes e mostrar quem pode mais, quem tem a melhor tecnologia.

A proteção dos dados está amparada pela legislação vigente, mas ainda tem que sair do papel e ser implementada nas empresas que não sabem o quão valioso é a base de dados das empresas, considero como um patrimônio da empresa e que exerce um peso sobre a acurácia de suas finanças e sobre o futuro dos seus negócios.

REFERÊNCIAS

- ANBC. **Associação Nacional dos Birôs de Créditos**. Disponível em: <https://anbc.org.br/o-que-e-um-biro-de-credito/>. Acesso em: 01 out. 2021.
- ARGENTINA. **Lei nº 25.326 desde 2000**. Dispõe sobre Proteção de Dados Pessoais. Disponível em: http://www.jus.gob.ar/media/3201023/personal_data_protection_act25326.pdf. Acesso em: 01 jun. 2021.
- BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Disponível em: www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 01 set. 2021.
- BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Lei do Cadastro Positivo. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 5 set. 2021.
- BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Lei de Acesso à Informação. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 10 set. 2021.
- BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 set. 2021.
- BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Disponível em: www.planalto.gov.br/ccivil_03/LEIS/L8078.htm. Acesso em: 01 set. 2021.
- BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 jul. 2021.
- BVS/SCPC. **Boa Vista Serviços SCPC**. Disponível em: <https://www.boavistaservicos.com.br/protacao-de-dados>. Acesso em: 01 out. 2021.
- CHILE. **Lei nº 19.628 desde 1999**. Dispõe sobre Proteção de Dados. Disponível em: <https://www.bcn.cl/leychile/navegar?idNorma=141599>. Acesso em: 09 set. 2021.
- DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. São Paulo: Thomson Reuters Brasil, 2019.
- ESTADOS UNIDOS DA AMERICA. **Dispõe sobre a Lei de Proteção da Privacidade de Crianças. 2021**. Disponível em: <https://www.ecfr.gov/cgi-bin/text->

idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5.
Acesso em: 09 set. 2021

ESTADOS UNIDOS DA AMÉRICA. **Lei ECPA. 1986**. Dispõe sobre a Privacidade de Comunicação eletrônica. Disponível em: <https://www.bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#electronic-communications-privacy-act-of-1986-ecpa-18-u-s-c-%C2%A7%C2%A7-2>. Acesso em: 10 set. 2021.

GREENWALD, Glenn; MACASKILL, Ewen; POITRAS, Laura. Edward Snowden: the whistleblower behind the NSA surveillance revelations. **The Guardian**, 11 jun. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Acesso em: 09 set. 2021.

O DILEMA das Redes. Diretor Jeff Orlowski / produtora Larissa Rhodes. **Netflix**, 2020.

RODRIGUES, Silvio. **Direito civil**: direito de família. São Paulo: Saraiva, 2002.

SERASA EXPERIAN. Disponível em: <https://www.serasaexperian.com.br>. Acesso em: 01 out. 2021.

SPC BRASIL. Disponível em: <https://spcbrasil.org.br/lgpd/politicas.html>. Acesso em: 01 out. 2021.

TARTUCE, Flávio. **Manual de direito civil**: volume único. 7. ed. Rio de Janeiro: Forense; São Paulo: Método, 2017.

UNIÃO EUROPÉIA. **Dispõe sobre Proteção de Dados, concomitante à Regulação Geral de Proteção de Dados**. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/pt/TXT/?qid=1559291025147&uri=CELEX:32016R0679#d1e40-1-1>. Acesso em: 09 set. 2021.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890.