UM ESTUDO SOBRE A PERCEPÇÃO DE SEGURANÇA QUE AS LEIS DIGITAIS EXERCEM SOBRE USUÁRIOS DE SERVIÇOS E PRODUTOS DIGITAIS

Data de aceite: 02/05/2023

Nathan Novais Borges
Universidade Presbiteriana Mackenzie - (IC)

Fabio Silva Lopes
Universidade Presbiteriana Mackenzie - (Orientador)

RESUMO: Leis que abrangem o contexto digital em relação à proteção de Dados vêm se tornando cada vez mais comuns, tais como a brasileira LGPD (Lei Geral de Proteção de Dados) e a GDPR (General Data Protection Regulation). A criação de regulamentações de manipulação e coleta de dados, que abrangem o contexto digital, são consequência da crescente expansão do mundo digital junto ao aumento exponencial na produção de dados. O principal objetivo de tais legislações é regulamentar o armazenamento, processamento e utilização de dados pessoais, com o intuito de proteger e garantir a segurança dos titulares desses dados. Porém muitos indivíduos possuem deficiências no que se refere ao conhecimento de Leis que abrangem o contexto digital e boas práticas sobre o comportamento e vivência dentro do mundo virtual, criando vulnerabilidades de segurança para tais pessoas. Entre os principais fatores que aceleraram a adoção de serviços computacionais por pessoas com menor familiaridade com a tecnologia, podemos citar a pandemia internacional de covid-19, que ao criar um cenário de mudança de comportamento da sociedade visando um maior distanciamento social, gerou tanto um aumento em interações através dos meios digitais quanto uma escalada no número de golpes digitais. Com base nesse cenário, esse estudo busca entender como os indivíduos, cada vez mais associados a um contexto digital, compreendem e entendem as Leis digitais, criadas para protegê-los.
PALAVRAS-CHAVE: Leis de Regulação de Dados, Segurança de Dados, Cidadão Digital

ABSTRACT: Laws covering the digital context in relation to Data protection have become increasingly common, such as the Brazilian LGPD (Lei Geral de Proteção de Dados) and GDPR (General Data Protection Regulation). The creation of data handling and collection regulations, which cover the digital context, are a consequence of the growing expansion of the digital world along with the exponential increase in data

production. The main purpose of such legislation is to regulate the storage, processing and use of personal data in order to protect and ensure the safety of the holders of such data. However, many individuals have deficiencies regarding the knowledge of Laws that cover the digital context and good practices on behavior and experience within the virtual world, creating security vulnerabilities for such people. Among the main factors which have accelerated the adoption of computer services by people with less familiarity with technology, we may mention the international pandemic of covid-19, which, by creating a scenario of change in society's behavior aiming at a greater social distance, has generated both an increase in interactions through digital means and an escalation in the number of digital scams. Based on this scenario, this study seeks to understand how individuals, increasingly associated to a digital context, understand and comprehend the Digital Laws, created to protect them.
KEYWORDS: Data Regulation Laws, Data Security, Digital Citizen

1 I INTRODUÇÃO

A Lei Federal n° 13709, de 14 agosto de 2018, mais conhecida como LGPD (Lei Geral de Proteção de Dados) (Brasil, 2018), entrou em vigência em setembro de 2020, inspirada em legislações internacionais, como a europeia GDPR, que vêm se tornando cada vez mais comuns no cenário mundial.

A Lei em seu Artigo 1°,

> "...dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (Brasil, 2018).

Portanto, a Lei foi criada para regular o tratamento e coleta de dados, que são produzidos de forma abundante todos os dias por diversos tipos de usuários, oferecendo maior segurança digital para as pessoas. Levando em conta o crescimento exponencial da produção de dados, reforçado pela aceleração da digitalização do mundo desde 2020, a LGPD mostrou-se um divisor de águas no contexto digital brasileiro.

Ademais a pandemia internacional de COVID-19, acelerou veementemente a digitalização de diversos processos, tanto para os usuários já acostumados ao uso cotidiano da tecnologia quanto para aqueles que possuíam pouca ou nenhuma familiaridade às ferramentas e processos digitais.

Ao relacionar a evolução significativa da capacidade de extração e análise de dados, junto a um crescimento no número de usuários pouco familiarizados ao contexto computacional, cria-se um cenário frágil para com a segurança e privacidade do usuário, que muitas vezes não compreende os seus direitos garantidos pela Lei que abrange o mundo digital. Dessa forma, torna-se importante compreender os riscos de segurança dentro do ambiente digital que tal conjuntura pode proporcionar ao usuário, e qual o nível de entendimento deles para com os seus direitos e responsabilidades conforme a Lei

estabelecida.

Portanto, o objetivo deste estudo será entender melhor a percepção das pessoas com relação à LGPD, considerando os impactos para a sociedade em um contexto de inserção digital crescente.

Assim, esse trabalho foi estruturado da seguinte forma: Referencial Teórico, com o objetivo de realizar uma revisão bibliográfica e um estudo com estudos e conceitos que contemplem este estudo; Metodologia, em que os métodos e abordagens adotados neste estudo são detalhados; Resultados e Discussão, em que são apresentados os dados e resultados adquiridos a partir do escopo definido dentro da metodologia, e realizada uma análise das informações adquiridas junto ao conhecimento adquirido a partir do Referencial Teórico; Considerações finais, em que os principais tópicos são retomados junto a uma conclusão do estudo realizado.

2 | REFERENCIAL TEÓRICO

2.1 Histórico das Leis De Proteção de Dados

2.1.1 Declaração dos Direitos dos Direitos – 1948

A regulamentação e proteção de informações pessoais é uma questão que a muito tempo vem sendo debatida. Porém, a partir da Declaração dos Direitos dos Direitos Universais do Homem, criada pela ONU em 1948, o assunto passou a ter uma maior relevância.

O seu artigo XII prevê a proteção do direito à privacidade “Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.”

Em 1950, a Convenção Europeia dos Direitos Humanos, buscou reafirmar a proteção do mesmo direito em seu artigo 8º. Porém, mesmo sendo um avanço significante em relação ao direito da privacidade, é importante perceber que nesse momento inicial, o artigo 8° afirma que esse direito poderia sofrer violações por parte de uma autoridade pública, conforme as situações listadas. Ademais, não fica claro como e por quem essa proteção em relação à privacidade deveria ocorrer e ser garantida.

2.1.2 Diretiva 95/46/CE – 1995

A Diretiva Europeia de 1995 é outro marco na história da regulação da proteção de dados. Lançada em uma época em que a internet e a digitalização dos serviços começavam a se consolidar cada vez mais, a Diretiva foi criada para ser utilizada dentro dos países membros da União Europeia (UE), podendo servir de exemplo também para os

não membros.

Ela tinha como objetivo regulamentar a coleta, formatação, utilização dos dados pessoais, sendo que aqui os dados pessoais podem ser definidos como “qualquer informação relativa a uma pessoa singular identificada ou identificável”, sendo “considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos de sua identidade física, fisiológica, psíquica, econômica, cultural ou social”.

Outra definição importante que a Diretiva traz é a de dados pessoais sensíveis, definidos como “dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual”.

A Diretiva 95/46/CE demonstrou ser de severa importância para com a época em que foi adotada, definindo não apenas a regulação de dados dentro da própria União Europeia. Estabeleceu a necessidade de que empresas atuantes no território europeu deveriam garantir a proteção dos dados pessoais ao enviar dados pessoais ao exterior da União Europeia, caso contrário, poderiam estar violando a Diretriz e criar problemas jurídicos.

2.1.3 GDPR (General Data Protection Regulation) – 2016

A Diretiva 95/46/CE que vigorava desde 1995, não foi capaz de acompanhar o ritmo crescente de expansão do mundo digital junto ao crescimento na produção de dados. Nesse contexto, começou a ser discutida uma revisão em relação à Diretiva.

Em 2016, a União Europeia aprovou a GDPR, General Data Protection Regulation, que representou um marco em relação às regulamentações sobre a utilização dos dados pessoais. A Lei tem como objetivo regulamentar o armazenamento, processamento e utilização de dados pessoais na União Europeia.

A Diretiva, utilizada como base para a criação da nova regulação de dados europeia, vigorou até o dia 24 de maio de 2018, sendo substituída pela GDPR em 25 de maio de 2018. Diferente da Diretiva, a GDPR é um Regulamento, devendo ser adotada em todos os membros da UE.

Em comparação à Diretiva anterior, a GDPR apresentou mudanças significativas, trazendo a introdução de novos direitos individuais, tais como: o direito do esquecimento, em que os dados do titular armazenados por uma organização, devem ser apagados em caso de solicitação do titular; o direito da portabilidade, que garante o direito do titular a exigir a transferência de seus dados de uma empresa para outra; a introdução de notificação obrigatória em casos de vazamentos de dados; a necessidade de existir um responsável pela proteção de dados; a aplicação de multas e penalidades em casos de violação da Lei.

Dessa forma, a GDPR, que visa garantir a segurança dados pessoais ao regulamentar como tais dados podem ser manipulados e coletados pelas empresas, está servindo como

referência para criação de outras legislações referentes à proteção de dados, como por exemplo a LGPD no contexto brasileiro.

2.1.4 LGPD (Lei Geral de Proteção de Dados) - 2018

A legislação brasileira até então, previa a proteção de dados pessoais em algumas normas internas. É possível citar:

(i) 1988 - Constituição Brasileira Federal - art. 5º- § 10°: "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", ou seja, a vida privada da pessoa natural é protegida pela Constituição, sendo passível de indenização caso venha a ser violada";

(ii) 1990 - Código de Defesa do Consumidor - art. 43°- "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.";

(iii)2014 Marco Civil da Internet – Busca estabeler garantias, principios e deveres em relação à utilização de internet no Brasil.

Entretanto, tais normas não estabeleciam uma regulação clara e objetiva em relação à manipulação e proteção de dados pessoais, fator necessário em uma condição crescente de produção de informações através de dados. Patricia Peck, em seu livro "Proteção de dados pessoais: comentários à Lei N. 13.709/2018, elabora:

> "A LGPD surge com o intuito de proteger direitos fundamentais como privacidade, intimidade, honra, direito de imagem e dignidade. Pode-se pontuar também que a necessidade de leis específicas para a proteção dos dados pessoais aumentou com o rápido desenvolvimento e a expansão da tecnologia no mundo, como resultado dos desdobramentos da globalização, que trouxe como uma de suas consequências o aumento da importância da informação. Isso quer dizer que a informação passou a ser um ativo de alta relevância para governantes e empresários: quem tem acesso aos dados, tem acesso ao poder."

Nesse contexto, a LGPD (Lei Geral de Proteção de Dados) foi aprovada em agosto de 2018, entrando em vigor a partir de agosto de 2020, buscando trazer um cenário nacional com maior segurança digital.

A Lei brasileira em seu artigo 5º traz importantes definições de termos e conceitos. A seguir, estão alguns termos definidos pela Lei, que são amplamente abordados neste estudo:

(i) dado pessoal - informação relacionada a pessoa natural identificada ou identificável;

(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;

(iii) consentimento - manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

A adoção da LGPD é prevista para qualquer caso de manipulação de dados que ocorra em território brasileiro, ou seja, mesmo que a operação de tratamento seja realizada fora de território nacional, caso os dados tenham sido coletados no Brasil, a aplicação da Lei é válida. A aplicação da GDPR é realizada de forma semelhante no âmbito europeu, fazendo com que dados coletados dentro União Europeia devam ser manipulados seguindo a Lei europeia.

Outro fator essencial a ser entendido é o consentimento do titular dos dados. A Lei prevê o consentimento específico e em destaque, entendendo que o titular é aquele que pode permitir a coleta e manipulação de seus dados.

O tratamento de dados deve estar de acordo com requisitos estabelecidos pela Lei. Segundo Patricia Peck (2018) "A LGPD destaca que o tratamento de dados pessoais deve observar a boa-fé e possuir finalidade, limites, prestação de contas, garantir a segurança por meio de técnicas e medidas de segurança, assim como a transparência e a possibilidade de consulta aos titulares.". Nesse tópico, é possível analisar uma diferença notável entre a legislação europeia e brasileira. A GDPR, em comparação à LGPD, elabora de forma mais detalhada e clara os requisitos a serem seguidos para a realização do tratamento dos dados pessoais.

Diversas empresas buscaram se adaptar para entrar nos padrões da LGPD, e dessa forma, buscam compreender a Lei. Porém, o cidadão comum, muitas vezes não compreende os próprios direitos digitais que a Lei garante. Um problema que existe na cultura digital dos usuários, que é por si só muito limitada, a ponto de não entenderem os próprios direitos e responsabilidades em um mundo online que está cada vez mais presente.

2.2 Aumento na utilização da internet

A LGPD não foi o único fator importante na experiência digital em 2020. A pandemia internacional de COVID-19, que o Brasil vem enfrentando desde março de 2020 foi um dos fatores que mais influenciou em uma maior vivência digital por parte de toda a população.

Segundo a pesquisa realizada pela ABComm (Associação Brasileira de Comércio Eletrônico) com o Movimento Compre & Confie, o faturamento cresceu cerca de 56.8% nos 8 primeiros meses de 2020, assim como o número de transações digitais que cresceu por volta de 65.7%. Portanto pode-se observar que diversos processos foram digitalizados, além disso muitas pessoas, que não possuíam familiaridade com ferramentas digitais, entraram em uma situação de aprender rapidamente a como se portar em um mundo digital, experiência que na maior parte das vezes é delicada.

A situação descrita acima foi observada pela pesquisa da Cetic.br, que identificou

um aumento relevante no número de compras online pelas classes C, com aumento de 37% para 64%, e nas classes D e E com aumento de 18% para 44%. Ou seja, pessoas com menor escolaridade e menor familiaridade com o mundo online, em um curto espaço de tempo, começaram a migrar para um ambiente digital.

Ademais, em uma condição na qual a utilização da internet é crescente por parte dos usuários, concomitantemente está ocorrendo um aumento na produção de dados e novas formas de extrair valor e relacionamento a partir deles. Neste cenário é capaz de observar o fenômeno que ficou conhecido como Big Data, caracterizado pela alta velocidade de processamento, volume e variedade de dados e informações armazenadas em bancos de dados, podendo ser definido como "[...] a capacidade de uma sociedade de obter informações de maneiras novas a fim de gerar ideias úteis e bens e serviços de valor significativo. Assim, a verdadeira revolução não está nas máquinas que calculam dados, e sim nos dados em si e na maneira como usamos" (MAYER-SCHÖN- BERGER; CUKIER, 2013).

Ao relacionar a rápida evolução da tecnologia de extração, processamento e análise de dados junto à falta de transparência em relação a forma como tais dados são tratados e manipulados, criam-se situações potencialmente nocivas àqueles que disponibilizam seus dados pessoais, assim "[...] a combinação de dados aparentemente inofensivos provenientes de diversas bases ou a análise de grandes bases de dados pode gerar informações potencialmente perigosas para indivíduos, organizações e até mesmo estados, e isso é difícil de prever com suficiente antecipação"(Breternitz, Vivaldo & Lopes, Fabio & Silva, Leandro, 2013).

O Artigo "Malice Domestic: The Cambridge Analytica Dystopia", escrito por Hal Berghel, aborda o escândalo da Cambridge Analytica, que foi acusada de interferir nas eleições presidenciais de 2016 nos EUA, ao utilizar da má prática de compartilhamento de dados praticada pelo Facebook.

Os dados gerados pelos usuários e compartilhados pelo Facebook e outras fontes, foram usados para catalogar o perfil dos eleitores e direcionar propagandas e materiais pró Trump e mensagens contrárias à candidata Hillary Clinton. Entre os dados utilizados para esta estratégia, estavam nomes, profissões, contatos, local de moradia, locais frequentados, e hábitos. Tais dados foram coletados sem o conhecimento dos usuários e posteriormente utilizados para influenciar os próprios eleitores.

É possível traçar um paralelo entre a passagem descrita acima e o artigo "What is data justice? The case for connecting digital rights and freedoms globally", da autora Linnet Taylor. Nesse artigo é abordada a ideia de "direito de dados" que determina caminhos éticos a serem tomados em um mundo de dados.

Segundo a autora, a manipulação e monitoramento das pessoas se torna cada vez mais assertiva, uma vez que as junções entre bases de dados tornam-se cada vez mais apuradas. Tais características tendem a ferir direitos de privacidade da população e abre

a discussão sobre o quão correto é utilizar-se de tais dados, muitas vezes gerados sem consentimento do público.

Assim, é criado um quadro de fragilidade para com a segurança digital dos usuários, ao relacionar fatores como, a expansão do ambiente digital no cotidiano, a necessidade da adoção de ferramentas digitais, agregados à rápida evolução da tecnologia, em contraste a um desenvolvimento mais lento e gradual da percepção dos usuários sobre os riscos relacionados à disponibilização de seus dados.

2.3 Vigilância com os dados

A crescente interação entre as pessoas e o ambiente digital se deu por diversos fatores, entre eles, a pandemia da COVID-19. A mudança de comportamento da sociedade visando um maior distanciamento social, gerou um aumento em interações através dos meios digitais. Com a utilização e dependência crescente dos serviços de Tecnologia da Informação, pôde-se observar o aumento de ataques cibernéticos.

Em um relatório chamado Fraud & Abuse Report, realizado pela empresa norte-americana Arkose Labs que é especializada na área de segurança da informação, o Brasil figurou entre os top 5 países com mais fraudes virtuais. Foi observado um grande aumento de fraudes em e-commerces, setor de jogos online e ataques contra dispositivos utilizados para trabalhar remotamente. Ou seja, todos os setores que receberam um maior fluxo de dados durante o período pandêmico, sofreram mais golpes virtuais.

Um grande exemplo de fraude digital ocorreu logo no início de 2021, um mega vazamento de dados que afetou mais de 200 milhões de brasileiros, o que gerou insegurança e desconfiança por parte da população por não saber o que foi vazado ou quem tem acesso a tais dados de forma clara. Entre tais dados, foram vazados CPFs, nomes, datas de nascimento, informações de veículos, CNPJs, entre outros. Tal vazamento faz com que diversos indivíduos estejam vulneráveis aos mais diversos crimes digitais.

Segundo Gordon e Ford (2006), crimes digitais podem ser separados em duas categorias, uma com foco na questão técnica e outra com foco no fator humano.

A primeira possui uma natureza mais técnica, podendo ser caracterizada por falhas de hardware ou software, e muitas vezes se tornam vulneráveis a ataques *hackers.* Nessa circunstância, a solução se dá através da mesma tecnologia, focando em questões de segurança, desde o planejamento até a implementação, visando softwares e hardwares mais seguros.

Um exemplo de falha técnica pôde ser visto logo ao início da pandemia. Em um contexto de isolamento social, plataformas de reunião virtual obtiveram uma grande aderência por parte das pessoas que buscavam novas formas de comunicação. Entre essas plataformas, a aplicação Zoom, foi destaque por demonstrar falhas de segurança digital. Em seu texto “PANDEMIA NA PANDEMIA: A ESCALADA DE ATAQUES CIBERNÉTICOS PÓS COVID-19” (2020), Nagli discorre: “Em um contexto de isolamento social, plataformas

de reunião virtual obtiveram uma grande aderência por parte das pessoas que buscavam novas formas de comunicação. Entre essas plataformas, a aplicação Zoom, foi destaque na grande mídia por demonstrar falhas de segurança digital.".

A segunda categoria, relacionada ao fator humano na interação entre pessoa e máquina, ocorre em diversos casos em que o usuário, por falta de conhecimento sobre os procedimentos corretos dentro do ambiente digital, cria brechas de segurança. Segundo o relatório "2021 Data Breach Investigations Report" (DBIR) da Verizon, cerca de 85% das violações de dados envolveram interações humanas, deixando clara a relevância do fator humano na segurança de dados. A solução nesse caso, se dá via a educação do indivíduo em relação à como interagir com o ambiente digital.

Quando se discute o tema comportamento das pessoas no mundo digital, o termo cidadão digital (digital citizen) torna-se importante para a discussão. Segundo Mike Ribble, 2011, cidadão digital pode ser definido como aquele que utiliza da tecnologia de maneira efetiva e apropriada.

Já a cidadania digital possui outra definição, segundo Searson, Hancock, Soheil, & Shepherd, 2015, a cidadania digital pode ser definida como o conjunto de qualidades exigidas para cidadãos utilizarem ferramentas digitais em diversos ambientes digitais de maneira adequada. No seu livro de 2015 "Digital Citizenship in Schools: Nine Elements All Students Should Know", Ribble elenca os nove elementos que compõem a cidadania digital. Entre esses fatores está a Segurança digital, definida pelo próprio autor como as precauções eletrônicas para garantir a segurança. Tal fator muitas vezes é ignorado, ao não se ler termos de contratos em sites e aplicações, não tomar os devidos cuidados com as senhas de segurança pessoais. Essas situações mostram-se curiosas, uma vez que no mundo físico o comportamento tende a ser o contrário, colocamos trancas e fechaduras nas portas, instalamos aparelhos de segurança em casa, câmeras de vigilância etc.

Junto da cidadania digital, está o termo digital literacy, que segundo Martin, pode ser definida como:

> "o conhecimento, atitude e habilidade dos indivíduos de usar apropriadamente ferramentas digitais para identificar, acessar, gerenciar, integrar, avaliar, analisar e sintetizar recursos digitais, construindo um novo conhecimento… habilitando ações sociais construtivas, e reflexão ao longo desse processo" (Martin,2006, p.155)

Tais conceitos como cidadania digital e digital literacy, estão relacionados diretamente à educação do indivíduo em relação à segurança no mundo digital. Assim, dentro de um contexto cada vez mais digital, cenário acelerado consideravelmente pela pandemia como abordado anteriormente, o tema da segurança não se encontra isolado ao restante da experiência digital dos usuários. Ademais, o entendimento da Lei, que abrange o contexto digital, também será parte fundamental a ser compreendida por todos, uma vez que traçar a linha tênue o que separa o mundo físico do virtual se torna progressivamente mais difícil.

3 | METODOLOGIA

A partir do cenário apresentado ao longo do referencial teórico, e considerando a carência de estudos relacionados ao nível da percepção de indivíduos para com as leis digitais, foi realizado um estudo exploratório, que de acordo com Gil (2012, p. 12), "têm como principal finalidade desenvolver, esclarecer e modificar conceitos e ideias, tendo em vista a formulação de problemas mais precisos ou hipóteses pesquisáveis para estudos posteriores". Desse modo, foram realizadas pesquisas bibliográficas relacionadas ao tema das Leis Digitais e temas relacionados ao seu contexto, visando compreender o nível técnico de informações disponíveis que auxiliassem a responder a pergunta "Qual o nível de percepção das pessoas em relação aos direitos e responsabilidades que a Lei Geral de Proteção de Dados impõe?".

A escolha da metodologia a ser utilizada foi a quantitativa. A metodologia quantitativa, de acordo com Lozada e Nunes, "utiliza instrumentos de coleta de dados estruturados, como questionários, para fazer a captação de dados, que são generalizados de uma amostra para toda uma população estudada". O estudo exploratório através da revisão da bibliografia, auxiliou na concepção das perguntas presentes dentro do formulário de pesquisa.

Com o intuito de entender as características e comportamentos dos indivíduos dentro do ambiente digital que é envolvido pela LGPD, um formulário de pesquisa foi criado utilizando a ferramenta Google Forms, aplicação criada pelo Google para criar e enviar formulários online, que ficou disponível para recepção de respostas ao longo de 29 dias, a partir do dia 30 de junho de 2022 até o dia 29 de julho de 2022.

Com as informações obtidas a partir do formulário, será realizada uma análise quantitativa dos dados através da construção e comparação de gráficos, buscando compreender e descrever a relação entre o comportamento do usuário dentro do ambiente digital e a sua compreensão sobre a Lei.

Desse modo, as perguntas foram divididas em duas seções: preliminar e comportamental.

A seção de qualificação do respondente tem como objetivo classificar os entrevistados com base na sua escolaridade, idade, localização e consumo de internet, buscando entender o perfil dos participantes.

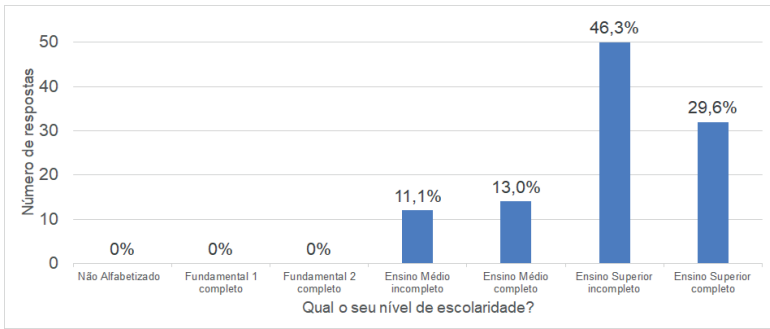
A seção comportamental possui perguntas que visam compreender o nível de percepção dos entrevistados em relação às Leis Digitais. Para compor parte das perguntas inseridas na seção comportamental do formulário e medir valores subjetivos, tais como a percepção, esse estudo utilizou a escala Likert, que "consiste em tomar um construto e desenvolver um conjunto de afirmações relacionadas à sua definição, para as quais os respondentes emitirão seu grau de concordância."(Júnior, Severino Domingos da Silva, and Francisco José Costa). (2014).

Os resultados deste estudo estarão sujeitos à limitação das respostas fornecidas pela população pesquisada. Dessa forma, a generalização dos dados obtidos a partir do formulário não garantem que os resultados sejam os mesmo em qualquer lugar, período ou outro grupo, que não o grupo de participantes analisados dentro deste estudo.

4 I RESULTADO E DISCUSSÃO

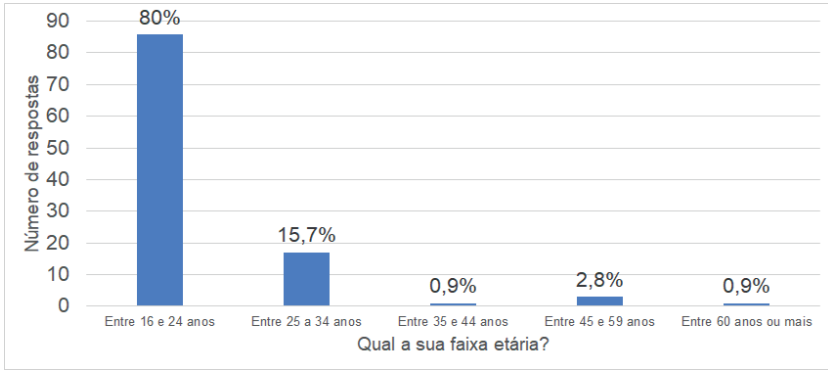
Com um total de 108 respostas coletadas ao longo de 29 dias, o questionário "Percepção sobre as Leis Digitais", entregou um recorte de como pessoas de faixas etárias e níveis de escolaridade distintos interagem dentro da internet, junto de como elas compreendem os riscos, benefícios, e segurança da disponibilização de seus dados.

Considerando todas as respostas, 11,1% dos participantes afirmaram ter o Ensino Médio Incompleto, já 13% afirmaram ter o Ensino Médio Completo, outros 46,3% informaram ter o Ensino Superior Incompleto e 29,6% disseram ter o Ensino Superior Completo.



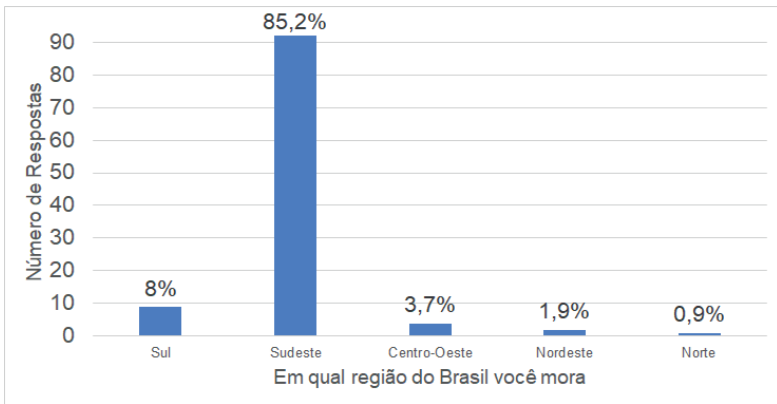
Pesquisa Qualidade Informações COVID19 – Pergunta: Qual o seu nível de escolaridade? [Figura 1]

Das 108 respostas coletadas, 79,6% dos participantes afirmaram ter entre 16 e 24 anos, já 15,7% disseram ter entre 25 e 34 anos, 0,9% informaram ter entre 35 e 44 anos, já 2,8% possuem entre 45 e 59 anos e outros 0,9% relataram ter 60 anos ou mais. Assim, 95,3% das pessoas envolvidas nesta pesquisa possuem entre 16 e 34 anos.



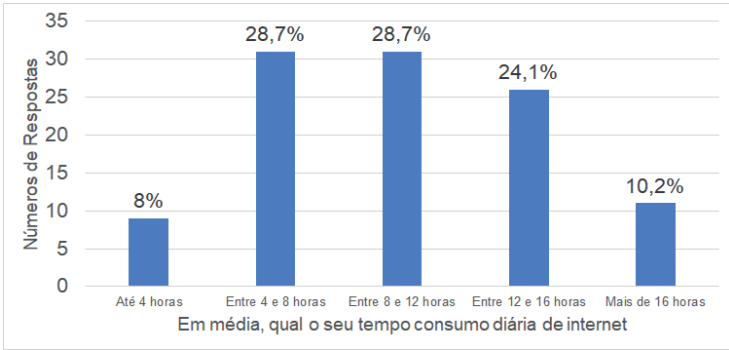
Pesquisa Qualidade Informações COVID19 – Pergunta: Qual a sua faixa etária? [Figura 2]

Aqueles que participaram do estudo também informaram a região na qual moram, e de acordo com os resultados obtidos, a maior parte dos participantes, representada por 85,2%, afirmaram morar no Sudeste, enquanto 8,3%, 3,7%, 1,9% e 0,9% disseram morar no Sul, Centro-Oeste, Nordeste e Norte, respectivamente.



Resultados: Pesquisa Qualidade Informações COVID19 – Pergunta: Em qual região do Brasil você mora? [Figura 3]

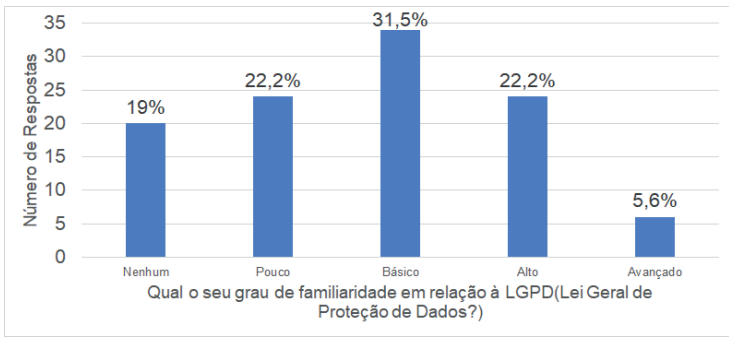
Buscando entender o nível de interação diária dos participantes com a internet, o questionário perguntou às pessoas qual o tempo médio de consumo diário de internet de cada. Em relação a essa questão, 8,3% dos participantes relataram ter um tempo médio de até 4 horas. O número de participantes que afirmaram ter entre 4 e 8 horas ou 8 e 12 horas de consumo diário de internet foi o mesmo, ambos 28,7%. Parte representada por 24,4% dos participantes disse usar a internet entre 12 e 16 horas, enquanto 10,2% responderam usar mais de 16 horas.



Pesquisa Qualidade Informações COVID19 – Pergunta: Em média, qual o seu tempo de consumo diário de internet? [Figura 4]

Após responder as perguntas preliminares, utilizadas para criar um perfil sociodemográfico, os participantes começaram a responder perguntas da seção comportamental, com o objetivo de entender o nível de percepção dos entrevistados em relação às Leis Digitais.

A primeira pergunta desta seção foi em relação ao grau de familiaridade das pessoas em relação à LGPD. Entre todos os participantes, 18,5% disseram ter nenhum conhecimento ou familiaridade com LGPD, já 22,2% afirmaram ter pouca familiaridade, 31,5% responderam básico, outros 22,5% consideraram sua familiaridade como alta e 5,6% disseram ter um grau de familiaridade avançado. Entre os que responderam ter uma alta familiaridade com a LGPD, a maior parcela é representada por aqueles que utilizam a internet de 12 a 16 horas, com um total de 33%.

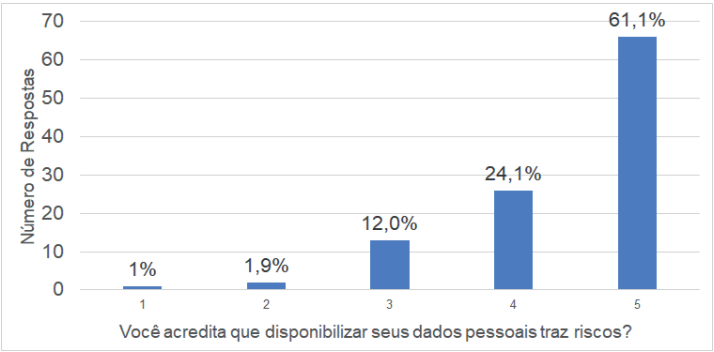


Pesquisa Qualidade Informações COVID19 – Pergunta: Qual o seu grau de familiaridade em relação à LGPD (Lei Geral de Proteção de Dados)? [Figura 5]

Após entender o grau de familiaridade em relação à LGPD, os participantes responderam perguntas relacionadas à disponibilização de seus dados pessoais, tópico central da Lei Geral de Proteção de Dados, com o objetivo de entender a percepção das

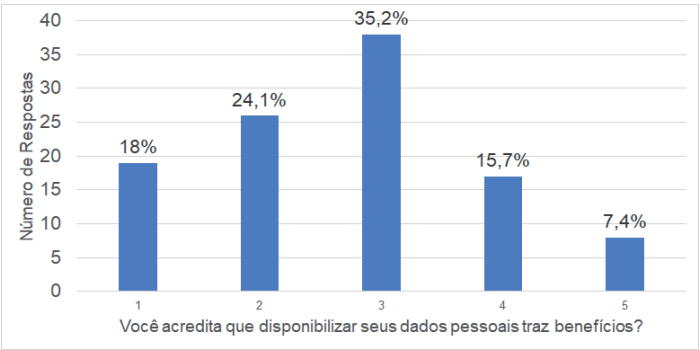
pessoas em relação aos riscos, benefícios e confiança na disponibilização de tais dados. Essas perguntas adotaram uma escala gradual de 1 a 5, tendo 1 como discordo totalmente e 5 como concordo totalmente.

Os participantes responderam à pergunta “Você acredita que disponibilizar seus dados pessoais traz riscos?”. A partir dessa pergunta foi possível observar que a maior parte dos entrevistados acreditam que a disponibilização de seus dados traz riscos, tendo 85,2% que responderam 4 ou 5, em contraste aos 2,7% que responderam 1 ou 2.



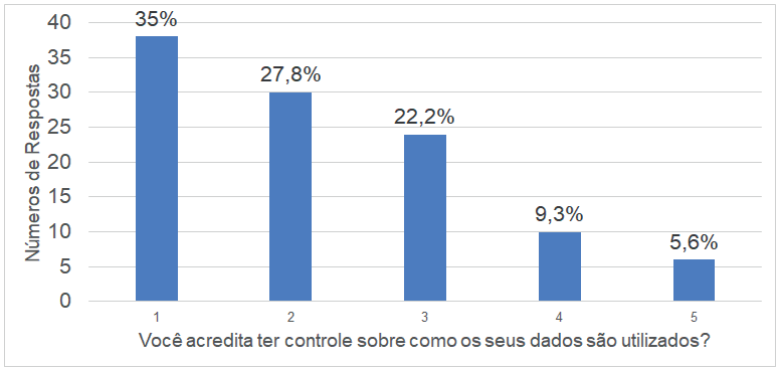
Pesquisa Qualidade Informações COVID19 – Pergunta: Você acredita que disponibilizar seus dados pessoais traz riscos? [Figura 6]

Os participantes também foram questionados com a pergunta “Você acredita que disponibilizar seus dados pessoais traz benefícios?”. Nesta pergunta os resultados foram mais equilibrados em relação à questão dos riscos, 41,7% responderam 1 ou 2, enquanto 23,1% assinalaram 4 ou 5 e um total de 35,2% selecionaram 3 como resposta. Apesar de um maior equilíbrio em relação à questão anterior, houve uma tendência maior de respostas contrárias à afirmativa de que disponibilizar dados pessoais traz benefícios.



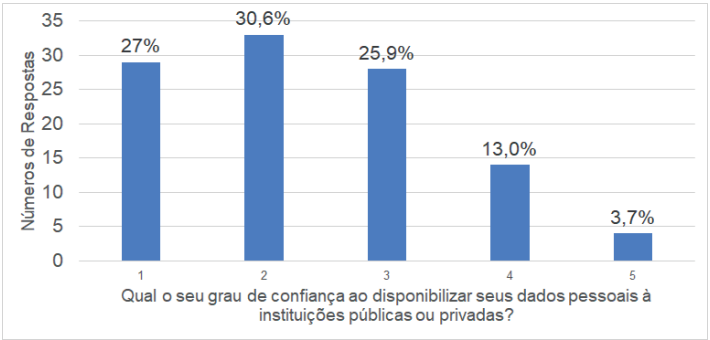
Pesquisa Qualidade Informações COVID19 – Pergunta: Você acredita que disponibilizar seus dados pessoais traz benefícios? [Figura 7]

Com o objetivo de compreender a percepção dos entrevistados em relação ao controle dos seus dados, foi realizada a pergunta “Você acredita ter controle sobre como seus dados são utilizados?”. Os participantes demonstraram uma maior discordância em relação à pergunta, sendo que 63% das pessoas responderam 1 ou 2, em contraste aos 11,9% que assinalaram 4 ou 5. Entre os participantes que disseram ter um nível de conhecimento “básico” em relação à LGPD, 70,6% afirmaram 1 ou 2, número maior em comparação ao total de respostas.



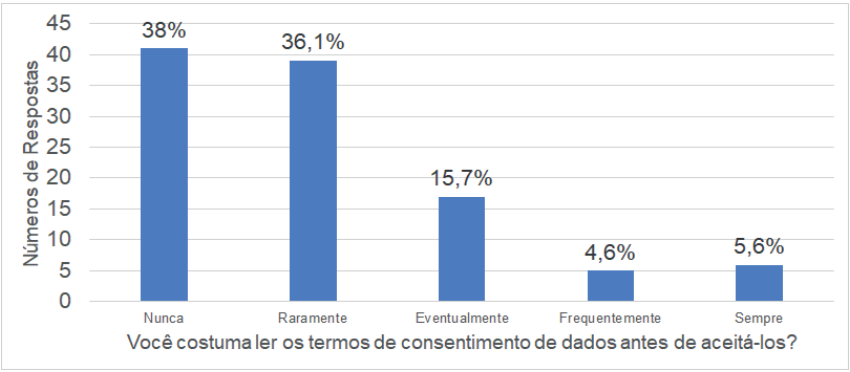
Pesquisa Qualidade Informações COVID19 – Pergunta: Você acredita ter controle sobre como os seus dados são utilizados? [Figura 8]

Os entrevistados também responderam à pergunta “Qual seu grau de confiança ao disponibilizar seus dados pessoais à instituições públicas ou privadas?”. As respostas deste item demonstraram uma tendência similar à pergunta anterior relacionada ao controle de seus dados pessoais, sendo que nessa questão os participantes também demonstraram uma tendência a um grau menor de confiança ao disponibilizar seus dados. 57,5% dos entrevistados responderam 1 ou 2, em oposição aos 16,7% que responderam 4 ou 5. Entre os participantes que disseram ter um nível de conhecimento “básico” em relação à LGPD, 64,7% afirmaram 1 ou 2, número maior em comparação ao total de respostas.



Pesquisa Qualidade Informações COVID19 – Pergunta: Qual o seu grau de confiança ao disponibilizar seus dados pessoais à instituições públicas ou privadas? [Figura 9]

Com o intuito de compreender como os participantes comportam-se diante de uma situação de disponibilização de dados pessoais, foi realizada a pergunta “Você costuma ler os termos de consentimento de dados antes de aceitá-los?”. Entre os 108 entrevistados, 38% dos participantes afirmaram nunca ler os termos de consentimento de dados, já 36,1% disseram ler raramente, 15,7% informaram que eventualmente realizaram essa leitura, enquanto 4,6% e 5,6% assinalaram frequentemente e sempre, respectivamente.



Pesquisa Qualidade Informações COVID19 – Pergunta: Você costuma ler os termos de consentimento de dados antes de aceitá-los? [Figura 10]

Portanto, ao longo da análise de resultados é possível notar que os entrevistados em sua maioria, tendem a acreditar que existem riscos ao disponibilizar seus dados pessoais, junto a uma falta de controle perante a tais dados. Porém, mesmo diante deste cenário pessimista em relação à disponibilização de dados, não possuem o hábito de realizar a leitura dos termos de consentimento de dados antes de aceitá-los, demonstrando uma contradição, uma vez que não ler tais termos diminui o conhecimento do indivíduo sobre quais dados serão disponibilizados e como serão tratados.