XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

CARLOS MARDEN CABRAL COUTINHO

JOSÉ RENATO GAZIERO CELLA

YURI NATHAN DA COSTA LANNES

D597

Direito, Governança e novas tecnologias I [Recurso eletrônico on-line] Organização CONPEDI

Coordenadores: Carlos Marden Cabral Coutinho; José Renato Gaziero Cella; Yuri Nathan da Costa Lannes. – Florianópolis: CONPEDI, 2023.

Inclui bibliografia
ISBN: 978-65-5648-813-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: Acesso à justiça, Solução de litígios e Desenvolvimento

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3; 2023; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

No XXX Congresso Nacional do CONPEDI, realizado nos dias 15, 16 e 17 de novembro de 2023, o Grupo de Trabalho - GT "Direito, Governança e Novas Tecnologias I", que teve lugar na tarde de 15 de novembro de 2023, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados 23 (vinte e três) artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente na Faculdade de Direito do Centro Universitário Christus - UNICHRISTUS.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva, os coordenadores do grupo de trabalho dividiram os artigos em cinco blocos, quais sejam a) temas de inteligência artificial; b) temas de liberdade de expressão e fake news; c) temas de proteção de dados pessoais; d) temas de cidadania, democracia, constituição e direitos; e e) temas de regulação.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema "Direito, Governança e Novas Tecnologias". Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. Carlos Marden Cabral Coutinho - Centro Universitário Christus

Prof. Dr. José Renato Gaziero Cella - Atitus Educação

Prof. Dr. Yuri Nathan da Costa Lannes - Faculdade de Direito de Franca

PROTEÇÃO DE DADOS PESSOAIS NOS AMBIENTES DIGITAIS MÉTODOS DE SEGURANÇA E PREVENÇÃO À LUZ DA LGPD

PROTECTION OF PERSONAL DATA IN DIGITAL ENVIRONMENTS: SECURITY METHODS AND PREVENTION CONSIDERING LGPD

Marília Marques Rodrigues
Fernando Freire Vasconcelos

Resumo

As discussões a respeito da proteção de dados pessoais não surgiram recentemente, mas ficaram populares com o advento da lei nº 13.709/2018 (LGPD). A lei tem por finalidade proteger os direitos fundamentais de privacidade, liberdade, desenvolvimento econômico, a livre iniciativa, bem como, os direitos humanos e o livre desenvolvimento da pessoa natural. Além disso, a LGPD estabeleceu algumas diretrizes para os agentes de tratamento de dados, como por exemplo, condutas de segurança, transparência e prevenção. E, também, deixou explícito quais são os direitos dos titulares de dados pessoais. Pontos relevantes para este projeto, visto que, como observa Davenport, o mundo está inundado de dados que se proliferam rapidamente (Davenport, 2014) e é difícil ter controle sobre todas as informações que cada indivíduo gera nos ambientes digitais. Por meio dessa pesquisa exploratória inicial, foi realizado um levantamento de dados sobre atividades de usuários no âmbito digital em relação aos próprios dados pessoais, buscando identificar se existe uma relação entre a faixa etária e os métodos utilizados para proteção. Também foi coletado dados sobre a Autoridade Nacional de Proteção de Dados (ANPD) em relação as suas atividades de fiscalização. Devido à natureza qualitativa dos dados, o método aplicado foi a análise de correspondência e observou-se que indivíduos entre 18 e 24 anos tendem a tomar medidas de segurança padrão médio, enquanto as pessoas com a faixa etária entre 25 e 30 anos tendem a tomar medidas de segurança padrão alto, ou seja, tomam mais medidas de segurança nos ambientes digitais.

Palavras-chave: Lgpd, Segurança, Dados pessoais, Titular dos dados, Agente de tratamento

Abstract/Resumen/Résumé

Discussions regarding the protection of personal data did not arise recently but became popular with the advent of law number 13.709/2018 (General Data Protection Law). The law aims to protect fundamental rights such as privacy, freedom, economic development, free enterprise, as well as human rights and the free development of natural persons. Additionally, the LGPD established some guidelines for data processing agents, such as security conduct, transparency, and prevention. It also made explicit the rights of data subjects. These are relevant points for this project, as Davenport observes that the world is awash with data that proliferate rapidly (Davenport, 2014) and it is difficult to have control over all the

information everyone generates in digital environments. Through this initial exploratory research, data was collected on users' digital activities related to their own personal data, seeking to identify whether there is a relationship between age group and the methods used for protection. Data was also collected on the National Data Protection Authority (ANPD) regarding its enforcement activities. Due to the qualitative nature of the data, correspondence analysis was applied, and it was observed that individuals between 18 and 24 years old tend to take medium standard security measures, while those aged 25 to 30 tend to take high standard security measures, meaning they take more security measures in digital environments.

Keywords/Palabras-claves/Mots-clés: Lgpd, Security, Personal data, Data subject, Data processing agent

1. INTRODUÇÃO

Diante do crescimento exponencial do uso de tecnologias e de mídias digitais, seja no setor público ou privado, hoje vivemos em um período digital, no qual sociedade encontra-se dependente das tecnologias da informação ou/e da comunicação no mundo todo. Com o crescimento da linguagem binária, a quantidade de dados processados e armazenados, bem como os riscos também cresceram em comparação à época que os papeis eram o principal meio de armazenagem de dados (BIONI, 2021).

Conforme pontua Davenport, o mundo está inundado de dados que se proliferam rapidamente, coletados, muitas vezes, para melhorias nas decisões do setor privado, público e na sociedade em geral (DAVENPORT, 2014). A ascensão do grande volume de dados ocorre em quase todas as áreas da sociedade, seja para contratos de trabalho até para receber indicações de compras (DAVENPORT, 2014).

Os dados pessoais movimentam novos modelos de negócios, principalmente quando é possível identificar seus titulares. O interesse por esses dados podem gerar situações de falhas de segurança, no qual terceiros podem utilizar os dados para as mais distintas finalidades (MULHOLLAND, 2020). O tratamento de dados pessoais realizado ou armazenado de forma indevida, pode gerar graves problemas para a população, um exemplo mais conhecido de violação de dados, é o escândalo da Cambridge Analytica, no qual a empresa comprou acesso a dados identificáveis da rede social Facebook, tendo acesso à cerca de 87 milhões usuários e os utilizou para a manipulação de eleições presidenciais (VÉLIZ, 2021).

Além disso, se os dados não são armazenados e tratados com segurança adequada, podem ficar vulneráveis a hackers que invadem sistemas e roubam dados pessoais para cometer fraudes, extorsão ou coação (VÉLIZ, 2021). Em 2020, no período de janeiro a março, a Arkose Labs analisou padrões de ataque em registros de contas, logins, pagamentos de serviços financeiros, comércio eletrônico, mídias sociais e jogos em diferentes países. Em seu relatório constatou que o Brasil se encontra entre os cinco países mais afetados por fraudes digitais (LABS, 2020).

Apesar dos crimes cibernéticos não serem considerados novidade, visto que se trata de um problema que surgiu na década de 1970 (PINHEIRO, 2020), veio a necessidade de uma regulamentação para a proteção de dados pessoais e coletivos a fim de proteger a população, os negócios empresariais e garantir a preservação dos direitos fundamentais (PINHEIRO, 2020).

Em 2016 se consolidou a promulgação do Regulamento Geral sobre a Proteção de Dados (RGPD) na União Europeia com o prazo de 2 (dois) anos para adequação, e tinha como finalidade proteção das pessoas físicas em relação ao tratamento e à circulação dos dados pessoais (PINHEIRO, 2020). Importante ressaltar, que durante esse período de 2 (dois) anos, as empresas interessadas em manter relações comerciais com os países da União Europeia deveriam ter uma legislação semelhante a RGPD, caso contrário, sofreriam com um tipo de barreira econômica (PINHEIRO, 2020).

No Brasil, já existiam legislações que tratavam da privacidade e proteção de dados pessoais de modo esparso, mas no ano de 2018 foi promulgada pelo presidente Michel Temer, a Lei de Proteção de Dados Pessoais (LGPD), entrando em vigência no ano de 2019. A lei nº 13.709/2018 (LGPD) é inspirada na RGPD, porém, um ponto emblemático é a diferença cultural entre o Brasil e a União Europeia. (RUARO et al., 2020).

A LGPD traz em seu texto diversos princípios que devem ser observados e, ainda, uma padronização do que antes estava espalhado pela legislação brasileira. A Lei Geral de Proteção de Dados tem por finalidade proteger os direitos fundamentais de privacidade, liberdade, desenvolvimento econômico, a livre iniciativa, bem como, os direitos humanos e o livre desenvolvimento da pessoa natural.

Conforme pontua Bioni (2022), a informação é o novo elemento estruturante de organização da sociedade, embora não seja apenas no ambiente virtual, e por isso a ciência jurídica deve se adequar e repensar suas categorias para os novos desafios regulatórios. Em complemento, Pinheiro (2020) destaca que as preocupações necessárias para o funcionamento de uma empresa passou a ser a aplicação de um Sistema de Gestão de Segurança da Informação, para que os processos empresariais internos estejam em segurança. Em razão disso, muitas empresas precisaram se adaptar as obrigações da nova lei, de forma parcial ou total.

Segundo dados do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC), 58,1% das empresas não possuem uma política de segurança digital, e 32,8% discutiram riscos de segurança digital com seus colaboradores (CGI/NIC, 2019).

Alguns métodos usados por empresas para manter a segurança dos bancos de dados é a criptografia, anonimização e pseudonimização dos dados, autenticação (TERADA, 2008), mas é necessário mais que isso, é preciso implementar um sistema de gestão e segurança (Pinheiro, 2020). Para os titulares dos dados, o Conselho Nacional do Consumidor em parceria com a Agência Nacional de Proteção de Dados, recomendam a

criação de backups, ativação de criptografia em unidades de armazenamento externa entre outras recomendações (ANPD, 2021).

Tendo em vista que a segurança digital e o tratamento de dados em conformidade com a Lei Geral de Proteção de Dados é uma realidade que deve ser implantada em todas as organizações que coletam e tratam dados, do contrário podem gerar prejuízos financeiros, implicações legais, interrupções operacionais e danos a reputação, é de suma importância a análise desse tema.

2. MATERIAL E MÉTODOS

Trata-se de uma pesquisa exploratória, pois, conforme conceitua Gil (2017), tem o propósito de proporcionar maior familiaridade com o problema, tornando-o mais claro e preciso a fim de construir hipóteses. O método de abordagem é considerado flexível, visto que envolve levantamento bibliográfico e documental, questionário e métodos de análise qualitativa de metadados.

A coleta de dados foi realizada em diversas plataformas, como pelo site da Autoridade Nacional de Proteção de Dados que diante de uma requisição justificada pela Lei de Acesso à informação disponibilizou alguns dados e através de um questionário realizado pela plataforma Google Forms. O Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil também foi uma fonte de coleta de dados.

A finalidade da coleta desses dados era realizar o tratamento, transformá-los em informações estatísticas padronizadas sobre, por exemplo, quantidade de denúncias por irregularidades no tratamento de dados, empresas que estão ou não adaptadas a LGPD, empresas que já nomearam encarregados, e que já tiveram os dados de clientes vazados.

O questionário foi desenvolvido com perguntas qualitativas e aplicado com a finalidade de realizar uma análise de associação entre a faixa etária e a preocupação com os próprios dados pessoais, se tomavam precauções para protegê-los e/ou se já tomaram conhecimento sobre ter seus dados vazados

Tratando-se de um estudo fenomenológico (GIL, 2017), foi preciso direcionar a pesquisa para atingir as variáveis de indivíduos que são usuários ativos da internet, seja para uso de redes sociais, compras ou consumir serviços de streamings e a faixa etária escolhida foi entre 18 e 51 anos. A faixa etária leva em consideração a mudança cultural que a tecnologia vem proporcionando, onde pessoas cada vez mais jovens estão tendo acesso a internet e as mídias digitais.

Além disso, existe um relatório realizado pela Pew Research Center que examinou o uso da internet e da tecnologia por diferentes gerações no ano de 2021 e constatou que as pessoas com idade entre 18 e 29 anos são menos atentos em relação a privacidade do que os as pessoas com idade entre 50 e 65 anos.

A figura 1 apresenta o fluxo das principais etapas do projeto de estudo:

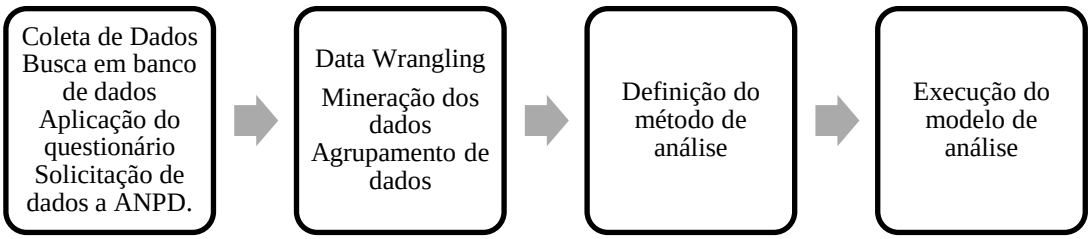


Figura 1 Etapas do estudo

Diante dos tipos de dados coletados, variáveis categóricas (qualitativas) não supervisionadas, considera-se a análise de correspondência como a técnica mais adequada. Conforme conceitua Fávero (2017) trata-se de uma análise simples, também chamada de Anacor, é uma técnica de análise bivariada utilizada para observar a associação ente variáveis categóricas e entre categorias a partir de um cruzamento de dados realizada a partir da estatística qui-quadrado (X^2).

O teste qui-quadrado é utilizado quando se pretende examinar se existe diferenças significativas nas proporções (prevalências) entre duas populações. Por exemplo, determinar se existe diferença entre as medidas de segurança utilizadas por pessoas de faixa etária entre 18 e 50 anos. O X^2 mede a diferença entre uma tabela de contingência observada e uma tabela de contingência esperada, partindo da hipótese de que não há associação entre as variáveis estudadas (FÁVERO, 2017).

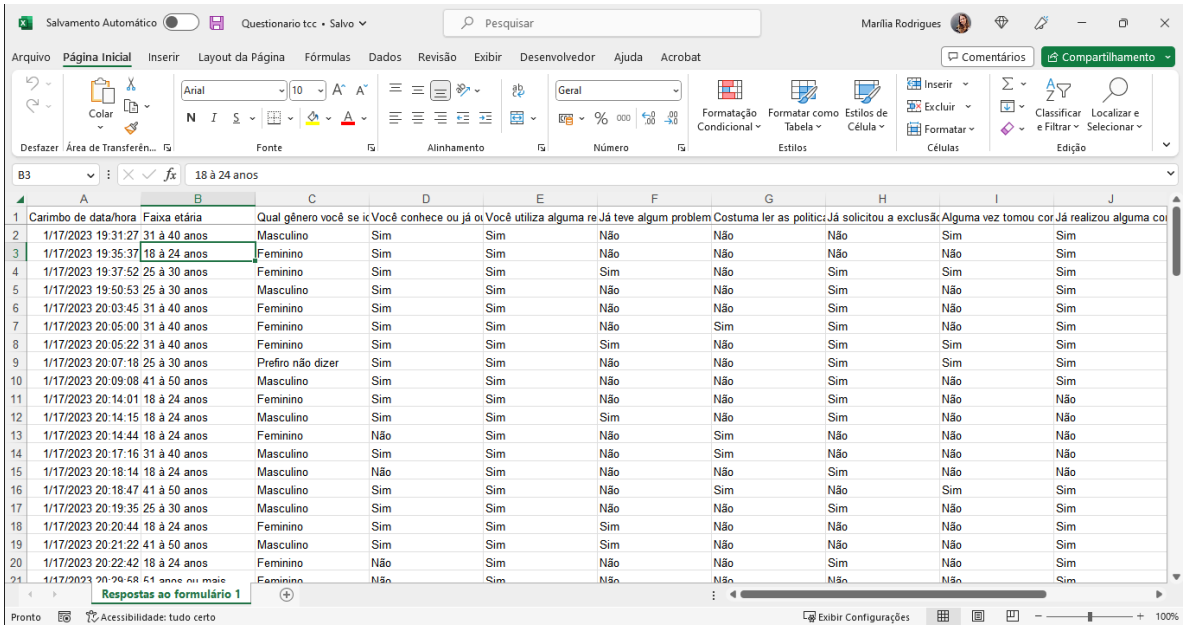
O principal objetivo da análise de correspondência simples é entender se existe uma associação estatisticamente significante a determinado nível de significância entre duas variáveis categóricas e entre as categorias de cada uma, conforme afirma Favero (2017).

O questionário foi aplicado da forma mais objetiva e simples possível, através da plataforma Google Forms, com o total de doze perguntas, com opções de respostas “sim” e “não”, sendo a última pergunta com seis opções de respostas podendo ser cumulativas. Todas as respostas foram recebidas de forma anônima, não tornando possível de identificar o voluntário da pesquisa, convém ressaltar ainda que, não foram coletados dados sensíveis de nenhuma natureza.

Conforme ressalta Gil (2017), na pesquisa qualitativa não é necessário selecionar uma amostra proporcional e representativa como ocorre em pesquisas quantitativas, mas levando em consideração que a estatística qui-quadrado (X^2) aumenta à medida que cresce o tamanho da amostra (FÁVERO, 2017), o objetivo era alcançar uma amostra com pelo menos 80 variáveis.

Foram recebidas 103 (cento e três) respostas, o que gerou uma tabela com 103 (centro e três) variáveis e 13 (treze) colunas, sendo 12 (doze) colunas referentes as perguntas e 1 (uma) referente a data e hora inserida automaticamente pela plataforma do Google.

A figura 2 traz uma parte da base de dados que foi gerada a partir das respostas do questionário:



Carimbo de data/hora	Faixa etária	Qual gênero você se id	Você conhece ou já ou	Você utiliza alguma re	Já teve algum problem	Costuma ler as politic	Já solicitou a exclusã	Alguma vez tomou cor	Já realizou alguma co
1/17/2023 19:31:27	31 à 40 anos	Masculino	Sim	Sim	Não	Não	Não	Sim	Sim
1/17/2023 19:35:37	18 à 24 anos	Feminino	Sim	Sim	Não	Não	Não	Não	Sim
1/17/2023 19:37:52	25 à 30 anos	Feminino	Sim	Sim	Sim	Não	Sim	Sim	Sim
1/17/2023 19:50:53	25 à 30 anos	Masculino	Sim	Sim	Não	Não	Sim	Não	Sim
1/17/2023 20:03:45	31 à 40 anos	Feminino	Sim	Sim	Não	Não	Sim	Não	Sim
1/17/2023 20:05:00	31 à 40 anos	Feminino	Sim	Sim	Não	Sim	Sim	Não	Sim
1/17/2023 20:05:22	31 à 40 anos	Feminino	Sim	Sim	Sim	Não	Sim	Sim	Sim
1/17/2023 20:07:18	25 à 30 anos	Prefiro não dizer	Sim	Sim	Não	Não	Sim	Sim	Sim
1/17/2023 20:09:08	41 à 50 anos	Masculino	Sim	Sim	Não	Não	Sim	Não	Sim
1/17/2023 20:14:01	18 à 24 anos	Feminino	Sim	Sim	Não	Não	Sim	Não	Não
1/17/2023 20:14:15	18 à 24 anos	Masculino	Sim	Sim	Sim	Não	Sim	Não	Não
1/17/2023 20:14:44	18 à 24 anos	Feminino	Não	Sim	Não	Sim	Não	Não	Não
1/17/2023 20:17:16	31 à 40 anos	Masculino	Sim	Sim	Não	Sim	Não	Não	Não
1/17/2023 20:18:14	18 à 24 anos	Masculino	Não	Sim	Não	Não	Sim	Não	Não
1/17/2023 20:18:47	41 à 50 anos	Masculino	Sim	Sim	Não	Sim	Não	Sim	Sim
1/17/2023 20:19:35	25 à 30 anos	Masculino	Sim	Sim	Não	Não	Sim	Não	Sim
1/17/2023 20:20:44	18 à 24 anos	Feminino	Sim	Sim	Sim	Não	Não	Não	Sim
1/17/2023 20:21:22	41 à 50 anos	Masculino	Sim	Sim	Sim	Não	Não	Não	Sim
1/17/2023 20:22:42	18 à 24 anos	Feminino	Não	Sim	Não	Não	Sim	Não	Sim

Figura 2: Tabela de dados gerados pelo questionário

Após a mineração dos dados, ficou estabelecido que os dados a serem considerados são: a faixa etária como faixa categórica e os métodos utilizados para a resguardo dos dados pessoais, com a finalidade de entender se indivíduos de uma determinada faixa etária está diretamente associada aos métodos de segurança utilizados diariamente no âmbito digital.

Foram escolhidos seis métodos de proteção de dados recomendados pela ANPD e pela Nation Cybersecurity Alliance, embora não exista um número fixo de medidas de segurança que possam ser considerados absolutamente seguros, visto que depende de

diversos fatores, como a atividade online, o valor das informações compartilhadas ou até ameaças específicas, podemos considerar mais vulnerável aqueles que utilizam menos ou nenhuma medida de segurança já que a segurança cibernética é uma prática em camadas.

Diante disso, para cada opção do questionário foi atribuído o valor 1, permitindo que cada pessoa pudesse selecionar até 6 opções. A quantidade das respostas classifica o método em seguro, médio ou em alto risco, sendo 1 e 2 pontos são considerados em risco, 3 e 4 pontos o nível de segurança é considerado médio, 5 e 6 é considerado seguro. As opções eram:

- → Utiliza senhas fortes
- → Mantém o antivírus sempre ativo e atualizado
- → Não compartilha dados confidenciais por mensagens e e-mails
- → Utiliza e-mails diferentes para contas importantes
- → Não abre e-mails ou links de desconhecidos
- → Utiliza cartão de crédito/débito temporário para compras online.

3. RESULTADOS E DISCUSSÃO

As opções de medida de segurança foram escolhidas dentro das recomendações da Autoridade Nacional de Proteção de Dados (ANPD), segundo a ANPD, considera-se senha forte aquela que contém palavras aleatórias, números, caracteres especiais e letras maiúsculas e minúsculas.

Ter o antivírus instalado, atualizado e ativo é importante para manter a segurança do computador e de dispositivos móveis.

Preservar a privacidade também exige atenção ao compartilhar arquivos, localização, fotos, porque uma vez que ocorre a postagem, difícil será seu desaparecimento completo, por isso não é recomendado compartilhar dados confidenciais sem estarem criptografados.

Alguns serviços oferecem a opção de utilizar conta externa para caso haja necessidade de autentificar, recuperar senha. É uma função importante porque permite a descentralização de apenas uma conta, pois em caso de comprometimento, todos os serviços relacionados a ela estarão em risco.

São usados links maliciosos com frequência com a intenção de direcionar os usuários para páginas falsas contendo malware ou até mesmo links com truques para

roubarem a conta. Por isso é importante não clicar em links desconhecidos e desconfiar de mensagens recebidas até mesmo por pessoas conhecidas.

Alguns bancos oferecem a opção de cartão temporário para realizar compras online, essa é uma medida de prevenção serve para prevenir que o usuário tenha seu cartão clonado e seus dados comprometidos.

3.1 Analise dos dados

O banco de dados apresenta duas variáveis categóricas, em que a primeira possui 5 (cinco) categorias, e a segunda, 3 (três) categorias. Diante disso, foi possível definir uma tabela de contingência a qual apresenta as frequências absolutas observadas das categorias das variáveis com uma classificação cruzada.

A tabela 1 é o ponto de partida para a realização da Anacor, representa o total das informações contidas no banco de dados, ou seja, os dados que podemos observar de forma empírica. Nessa tabela, ocorre o cruzamento das variáveis, por exemplo, 25 pessoas da faixa etária de 25 a 30 anos usam métodos seguros no ambiente digital.

Tabela 1. Frequência absoluta observada

	Nível de segurança			
Faixa Etária	Seguro	Médio	Risco	Total
18 à 24 anos	5	14	2	21
25 à 30 anos	25	18	9	52
31 à 40 anos	4	8	5	17
41 à 50 anos	3	3	1	7
51 anos ou mais	1	3	2	6
Total	38	46	19	**103**

Fonte: Resultados originais de pesquisa

A tabela 2 é a definição das frequências absolutas esperadas para cada par de categorias, ela é baseada nos somatórios das categorias em linha e em coluna, dividido pelo total da amostra.

Tabela 2. Frequências absolutas esperadas

	Nível de segurança		
Faixa Etária	Seguro	Médio	Risco
18 à 24 anos	7,75	9,38	3,87
25 à 30 anos	19,18	23,22	9,59
31 à 40 anos	6,27	7,59	3,14
41 à 50 anos	2,58	3,13	1,29
51 anos ou mais	2,21	2,68	1,11

Fonte: Resultados originais de pesquisa

A tabela 3 trata dos resíduos, os resíduos são a diferença entre as frequências absolutas observadas e as frequências absolutas esperadas. Nota-se que alguns valores de resíduos são negativos, isso ocorre porque o valor observado é menor que o valor esperado, já os valores positivos significa que os valores observados são maiores que o esperado.

Tabela 3. Resíduos

	Nível de segurança		
Faixa Etária	Seguro	Médio	Risco
18 à 24 anos	-2,75	4,62	-1,87
25 à 30 anos	5,82	-5,22	-0,59
31 à 40 anos	-2,27	0,41	1,86
41 à 50 anos	0,42	-0,13	-0,29
51 anos ou mais	-1,21	0,32	0,89

Fonte: Resultados originais de pesquisa

A existência dos valores de resíduos é o que determina a associação dessas categorias. Se os resíduos dessem o valor zero, significaria que a frequência absoluta observada e a frequência absoluta esperada são exatamente iguais, o que nos levaria a conclusão de que não há associação entre essas categorias (FÁVERO, 2017).

O cálculo dos resíduos são a base para a estatística qui-quadrado (X^2). O X^2 serve para verificar se há associação estatisticamente significante entre as variáveis qualitativas (Fávero, 2017). Para definir os valores da tabela 4, foi necessário definir o grau de liberdade primeiro porque a distribuição X^2 depende do parâmetro de graus de liberdade (FÁVERO, 2017). Sendo: (5-1)x(3-1) = 8.

Os valores X^2 referem-se a soma dos valores correspondentes à razão entre o resíduo elevado ao quadrado e a frequência esperada. Dados o nível de significância e os graus de liberdade, se o valor X^2 for maior do que seu valor crítico, há associação significante entre as duas variáveis (FÁVERO, 2017). A tabela 4 mostra que as variáveis são associáveis de forma significativa, mas ainda não é possível identificar a origem dessa associação.

Tabela 4. Valores X^2

	Nível de segurança		
Faixa Etária	Seguro	Médio	Risco
18 à 24 anos	0,97	2,28	0,91
25 à 30 anos	1,76	1,17	0,04
31 à 40 anos	0,82	0,02	1,11
41 à 50 anos	0,07	0,01	0,07
51 anos ou mais	0,67	0,04	0,72
		X^2 total	10,65
		p-valor	0,22

Fonte: Resultados originais de pesquisa

Para identificar a origem dessa associação, o próximo passo é identificar se há ou não ponto de associação significativa através da tabela 5 de resíduos padronizados. Os resíduos padronizados são relevantes porque permitem aprofundar a análise com foco nas categorias das variáveis (Fávero, 2017). Logo, observa-se o excesso ou falta de ocorrência de casos nas categorias das variáveis.

Tabela 5. Resíduos padronizados

	Nível de segurança		
Faixa Etária	Seguro	Médio	Risco
18 à 24 anos	-0,99	1,51	-0,95
25 à 30 anos	1,33	-1,08	-0,19
31 à 40 anos	-0,91	0,15	1,05
41 à 50 anos	0,26	-0,07	-0,26
51 anos ou mais	-0,82	0,20	0,85

Fonte: Resultados originais de pesquisa

A tabela 6 mostra os resíduos padronizados ajustados, conforme afirma Fávero (2017), se o valor do resíduo padronizado ajustado for maior do que 1,96, interpreta-se que existe associação significativa, ao nível de significância de 5%, entre as duas categorias que interagem na célula e se for menor do que 1,96, não há associação estatisticamente significativa.

Tabela 6. Resíduos padronizados ajustados

	Nível de segurança		
Faixa Etária	Seguro	Médio	Risco
18 à 24 anos	-1,39	2,27	-1,18
25 à 30 anos	2,38	-2,07	-0,30
31 à 40 anos	-1,25	0,22	1,28
41 à 50 anos	0,34	-0,10	-0,29
51 anos ou mais	-1,06	0,27	0,97

Fonte: Resultados originais de pesquisa

A figura 3 apresenta o mapa de calor, no qual é possível visualizar de forma mais clara os resíduos padronizados ajustados que são estatisticamente significantes:

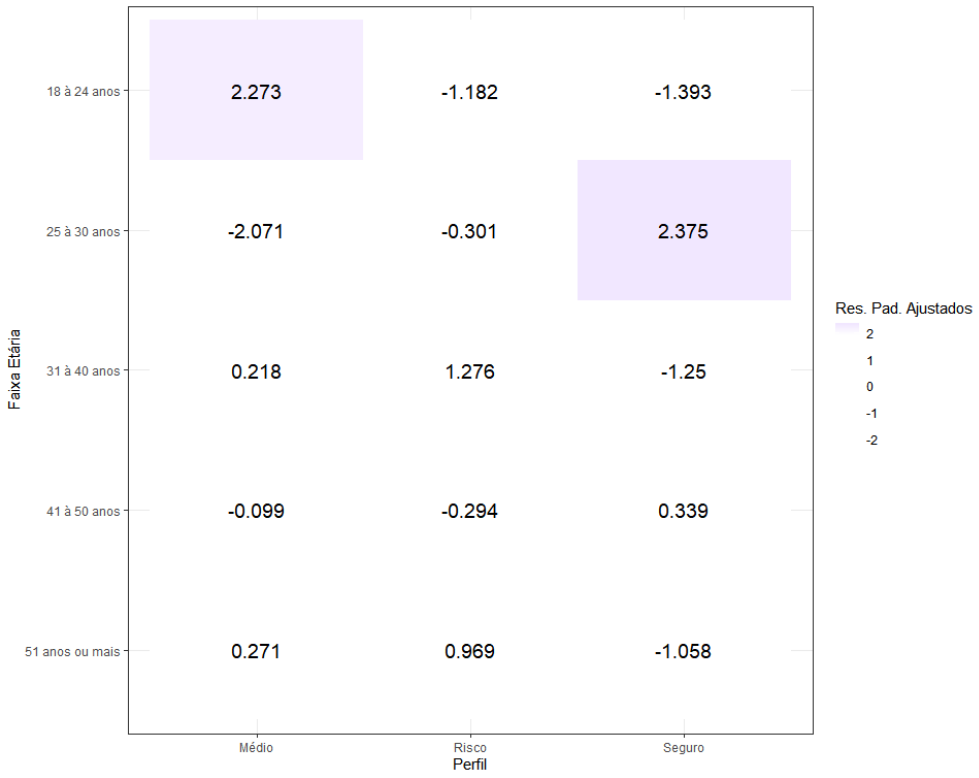


Figura 3: Mapa de Calor

Com base na análise de dados apresentados na tabela 6 e na figura 5, foi observado que aproximadamente 20,4% das pessoas na faixa etária de 18 a 24 anos adotam medidas de segurança considerado médio. Por outro lado, cerca de 48,08% das pessoas na faixa etária de 25 a 30 anos adotam medidas de segurança em um nível considerado seguro, indicando uma maior predisposição a se protegerem em ambientes digitais. As demais faixas etárias não apresentaram uma associação estatisticamente significativa com os níveis de medidas de segurança adotadas.

3.2 Dados Pessoais e Autoridade Nacional de Proteção de Dados

Conforme pontua Bioni, a informação é o atual elemento estruturante que organiza a sociedade, não apenas nos ambientes virtuais como nos ambientes físicos (BIONI, 2021). Principalmente no setor mercadológico, onde os bens de consumo e a publicidade utilizam dados como engrenagem da economia (BIONI, 2021). Em complemento, Doneda explica a técnica conhecida como *profiling*, essa técnica utiliza métodos estatísticos e inteligência artificial com a finalidade de obter uma "metainformação", que consiste em um apanhado dos hábitos, preferências pessoais e outros registros da vida de

uma pessoa ou de grupos. O resultado desse procedimento pode ser utilizado para decisões, comportamentos e influenciar o destino de um indivíduo ou grupo (DONEDA, 2020).

É necessário entendermos alguns conceitos relacionados a dados, informação, dados pessoais e dados pessoais sensíveis. De modo geral, os dados são registros que quando ordenados passam a transmitir significado (BIONI, 2021). Já a informação, segundo a lei de acesso à informação (LAI), é o agrupamento de dados processados ou não que podem ser utilizados para a produção de conhecimentos.

A lei geral de proteção de dados pessoais conceitua dados pessoais como informação relacionada a pessoa natural identificada ou identificável (Lei nº 13.709/2019). Já o artigo 5º, inciso II da LGPD traz o conceito de dados pessoais sensíveis, são dados relacionados a origem racial ou étnica, convicção religiosa, opinião pública, 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.

A legislação brasileira não foi a única que fez essa distinção, o regulamento geral de proteção de dados (RGPD) da União Europeia, proíbe o tratamento de dados pessoais relacionados a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa (LIMA, 2021).

A partir disso, Teixeira classifica dados pessoais em diretos e indiretos, o primeiro quando as informações identificam diretamente uma pessoa e o segundo é quando existe a possibilidade de a pessoa ser identificada pelas informações (TEIXEIRA, 2022). Importante ressaltar que a proteção dos dados pessoais não se dá pelo sigilo, mas pelo estabelecimento de procedimentos para o tratamento (BIONI, 2021).

A LGPD e a RGPD trouxeram regras especializadas em proteção de dados pessoais com a finalidade de instituir uma nova cultura de privacidade e proteção de informações pessoais (PINHEIRO, 2021). Sendo essa mudança cultural aplicável para os titulares dos dados e para os agentes de tratamento de dados pessoais. Para os titulares porque urge a necessidade de tornar seus direitos claros e conhecidos, e para os agentes porque passam a ter conhecimento sobre as regras para realização do tratamento de dados pessoais de forma ética e coerente (PINHEIRO, 2021).

O tratamento de dados deve observar a boa-fé, ser transparente e seguro, caso contrário, poderia pôr em risco a privacidade e a proteção dos dados pessoais (LIMA, 2021). De qualquer modo, a instituição de boas práticas em proteção de dados não se dá de maneira rápida, é um processo que leva tempo e investimento (PINHEIRO, 2021).

Sendo assim, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal com a finalidade de zelar pela proteção de dados, fiscalizar e implementar a lei geral de proteção de dados no território nacional (LIMA, 2021). As autoridades de proteção de dados têm sido consideradas instrumentos regulatórios fundamentais porque desempenham papeis de ouvidoria, auditoria, consultoria, de educação, de negociação, de aconselhamento político e executivo (LIMA, 2021). A importância da autoridade nacional de proteção de dados está relacionada à necessidade de uniformização dos entendimentos com a finalidade de proporcionar maior segurança jurídica na interpretação e aplicação da lei (LIMA, 2021).

Diante disso, outra fonte de dados importante para a realização do presente estudo foi a ANPD, a qual disponibilizou alguns dados sobre sua atuação na fiscalização e procedimentos administrativos no período de 2020 a 2022 diante de uma requisição feita com base na Lei de Acesso à Informação (LAI). A Autoridade Nacional de Proteção de Dados Pessoais informou que recebeu, desde dezembro de 2020 até setembro de 2022, 613 petições de titulares (das quais 294 foram arquivadas) e 976 denúncias (das quais 671 foram arquivadas), informou, ainda, que foram instaurados 25 procedimentos de fiscalização, dos quais 10 já foram concluídos e 15 estavam em trâmite até o momento da pesquisa, além de 8 processos administrativos sancionadores em curso (ANPD, 2022). Diante das informações prestadas, a tabela 7 mostra os dados recebidos pela ANPD organizados:

Tabela 7. Tabela de dados fornecidos pela ANPD

Período de dezembro de 2020 a setembro de 2022

Petições		Denúncias		Procedimentos de Fiscalização		Processos Administrativos	
Recebidas	613	Recebidas	976	Recebidos	25	Em curso	8
Arquivadas	294	Arquivadas	671	Concluídos	10		
				Em trâmite	15		

Fonte: ANPD

Segundo as informações da tabela 7, podemos concluir que a ANPD investigava na época 31% das denúncias recebidas e analisava cerca de 52% das petições recebidas. E que todos os procedimentos de fiscalização recebidos eram tramitados.

Embora tenha sido criado recentemente, a ANPD tem demonstrado um papel fundamental na proteção de dados pessoais, nota-se que ela vem trabalhando de forma ativa na fiscalização e aplicação das normas, com o intuito de garantir que empresas e organizações cumpram as obrigações previstas na lei. Além disso, a ANPD tem trabalhado em parceria com diversas instituições para desenvolver soluções e ferramentas que objetivam garantir segurança e privacidade dos cidadãos.

3.3 Segurança Organizacional

A propagação da cultura de segurança da informação é considerada valiosa e indispensável atualmente e está intimamente ligada a proteção de dados (GUERREIRO E TEIXEIRA, 2022). Em complemento, pontua Pinheiro que a aplicação de um Sistema de Gestão de Segurança da Informação (SGSI) é fundamental para o funcionamento de qualquer organização, principalmente porque ameaças cibernéticas cresceram e foram aprimoradas nos últimos anos (SLEIMAN...et al., 2021).

A segurança da informação conta com a norma ISO 27000, trata-se de um conjunto de padrões internacionais que estabelecem diretrizes e práticas para a gestão da segurança da informação em empresas e organizações (POHLMANN, 2021). Esses padrões são definidos pela International Organization for Standardization (ISO) e foram desenvolvidos com o objetivo de proteger as informações da empresa, considerando critérios de confidencialidade, integridade e disponibilidade (SLEIMAN...et al., 2021).

A confidencialidade se baseia na garantia de que a informação será restrita e armazenada de forma segura. A integridade busca garantir que a informação será conservada, ou seja, sem que haja qualquer tipo de manipulação não autorizada, por fim, a disponibilidade é a garantia que pessoas autorizadas tenham acesso às informações sempre que necessário (SLEIMAN...et al., 2021).

A norma ISO 27000 é aplicável a empresas de qualquer porte ou segmento, e é especialmente importante para aquelas que lidam com informações sensíveis, como dados de clientes (CHAGAS, 2020). A segurança da informação deve fazer parte da rotina da

organização, principalmente na dos colaboradores que tratam dados a fim de prevenir acesso não autorizado (GUERREIRO E TEIXEIRA, 2022).

Além disso, o mapeamento de dados pode ser considerado o alicerce no processo de adequação das empresas, pois esse procedimento consiste em identificar quais os tipos de dados pessoais são coletados e tratados na execução do negócio (PINHEIRO, 2021). Pinheiro recomenda que as informações devem ser classificadas em pública, interna e confidencial levando em consideração os possíveis impactos que seu vazamento poderiam causar (SLEIMAN...et al., 2021).

Pública porque seu compartilhamento pode ocorrer tanto no ambiente interno quanto no ambiente externo sem que haja problemas. Interna porque deve ficar restrita no ambiente da empresa e confidencial quando se tratar de alguma informação que apenas um grupo específico de colaboradores possam acessá-la (SLEIMAN...et al., 2021).

A norma ISO 27000 e a Lei Geral de Proteção de Dados (LGPD) são duas referências importantes quando se trata de proteção de dados e segurança da informação, uma das principais semelhanças entre a norma ISO 27000 e a LGPD é a ênfase na importância da proteção de dados pessoais e na adoção de medidas para garantir a segurança das informações (CHAGAS, 2020).

No entanto, a LGPD traz a definição de direitos dos titulares dos dados e as obrigações das empresas que coletam e tratam esses dados, a lei também estabelece requisitos específicos para o consentimento do titular, a transparência no uso dos dados e a comunicação em caso de vazamento ou incidentes de segurança. Enquanto a ISO 27000 é considerada uma referência mais ampla, que abrange até aspectos técnicos, não sendo específica para a proteção de dados pessoais, mas sim para a gestão da segurança da informação como um todo.

3.4 Sanções

A lei geral de proteção de dados pessoais traz em seu capítulo VII as medidas de segurança e as boas práticas que os agentes de tratamento devem adotar para proteger os dados pessoais. E é de suma importância que as organizações se adaptem, porque caso haja algum incidente a Autoridade Nacional de Proteção de Dados Pessoais irá realizar uma avaliação levando em consideração as medidas que foram tomadas para reverter ou diminuir o impacto do incidente (TEIXEIRA, 2022).

A aplicação de sanções dependerá do grau do dano e do tipo de vazamento, podendo ser da esfera administrativa, civil ou penal. São elas:

I. Advertência
II. Multa simples de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil
III. Multa diária
IV. Publicização da infração após devidamente apurada e confirmada a sua ocorrência
V. Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI. Eliminação dos dados pessoais a que se refere a infração;
VII. Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
VIII. Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
IX. Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Importante ressaltar que as sanções somente serão aplicadas após procedimento administrativo, no qual é respeitado o princípio da ampla defesa e devido processo legal (Lei nº 13.709/2018).

3.5 Riscos

Toda essa preocupação e cuidado em torno da proteção dos dados pessoais é justificável porque os dados pessoais de um indivíduo são informações que o identificam de alguma forma, como nome, endereço, número de telefone, e-mail, CPF, RG, por exemplo. E se houver algum incidente, como vazamento de dados, pode acarretar diversos tipos de consequências para o titular dos dados, como a utilização para fraudes e crimes, além da possibilidade de afetar a privacidade e causar danos a sua personalidade (TEIXEIRA, 2022).

Por tais razões, é importante que o cidadão esteja atento aos direitos sobre os próprios dados pessoais, tomando medidas preventivas para garantir que eles não sejam coletados ou utilizados de forma inadequada ou ilegal, como usar senhas seguras, não compartilhar informações pessoais com fontes não confiáveis, além de verificar regularmente suas contas e transações para detectar possíveis atividades suspeitas. Além disso, é importante que as empresas implementem medidas de segurança efetivas, como o uso de criptografia, autenticação de acesso, firewalls e backups, a fim de evitar o acesso não autorizado aos dados pessoais. Caso contrário, o titular pode estar sujeito a diversos riscos, como:

Roubo de identidade: criminosos podem utilizar os dados pessoais de um indivíduo para se passarem por ele, realizando compras ou transações financeiras em seu nome, causando prejuízos financeiros e danos à sua reputação.

Fraudes financeiras: com acesso a dados pessoais, criminosos podem abrir contas em bancos e instituições financeiras em nome da vítima, obter empréstimos e crédito em seu nome, ou ainda desviar recursos financeiros.

Vazamento de informações: empresas ou organizações que coletam dados pessoais podem ser alvo de ataques cibernéticos, resultando no vazamento dessas informações e colocando em risco a privacidade e segurança dos indivíduos afetados.

Spam e phishing: dados pessoais podem ser utilizados para enviar mensagens de spam ou e-mails fraudulentos (phishing), que buscam enganar a vítima para obter informações sensíveis, como senhas e dados financeiros.

3.6 Anonimização dos dados

É importante ressaltar que a lei geral de proteção de dados não protege dados anonimizados ou pseudonimizados, pois não são considerados dados pessoais (LIMA, 2021). O dado anonimizado é aquele que pertence a uma pessoa natural, mas não é possível identificá-la (POHLAMNN, 2021).

Inclusive, a anonimização dos dados é uma das recomendações que Bioni faz como método tecnológico aliado a proteção da privacidade. Esse processo envolver diferentes técnicas como a eliminação de informações diretas e indiretas de identificação pessoal, como nomes, endereços, números de telefone, CPF, e-mails e outros identificadores únicos. Também pode envolver a agregação de dados, substituição de

valores, supressão de informações sensíveis e outras técnicas para tornar os dados não identificáveis (BIONI, 2021).

No entanto, é importante destacar que a anonimização não é uma solução definitiva e que, em alguns casos, é possível reidentificar um indivíduo a partir dos dados anonimizados. Por isso, a LGPD estabelece regras específicas para a anonimização de dados pessoais, incluindo a necessidade de avaliação de risco, utilização de medidas técnicas e organizacionais adequadas e a observância de outras obrigações previstas na lei.

Como exemplo prático, temos a empresa de tecnologia Google, a organização utiliza o método de generalização dos dados que permite alcançar o k-anonimato, uma técnica que esconde a identidade dos indivíduos em um grupo de pessoas semelhantes. E adição de ruídos aos dados, uma técnica para adição de ruído matemático aos dados, isso faz com que o resultado de um algoritmo específico parecerá essencialmente o mesmo, independentemente de as informações dos indivíduos estarem incluídas ou omitidas (GOOGLE, 2023).

4. CONCLUSÃO

Hodiernamente a cultura da proteção de dados pessoais ainda está evoluindo, mas ainda não é compreendida por todos como mostrou o resultado da análise, o grupo da faixa etária de 25 a 30 anos demonstrou tomar mais precações para proteger os próprios dados nos ambientes digitais, enquanto os outros resultados foram mais baixos. Esses resultados contrastam com o estudo realizado pela Pew Research Center que havia constatado que as pessoas com idade entre 18 e 29 anos tendiam a ser menos vigilantes em relação a preservação da privacidade.

Por outro lado, a ANPD evidencia um compromisso ativo na fiscalização e aplicação das diretrizes estabelecidas pela LGPD, desempenhando um papel fundamental na política de proteção aos dados pessoais com o propósito de assegurar que empresas e organizações estejam em conformidade com as obrigações estipuladas pela lei.

É notório que estamos caminhando na direção certa, e muitas empresas têm se atualizado para se adequar às novas normas e leis, como a LGPD. Mas ainda há muito trabalho a ser feito para que a proteção de dados se torne uma prática comum e rotineira em todas as empresas e organizações.

O alinhamento da prática do tratamento de dados com a legislação é de extrema importância para garantir a segurança e privacidade das informações pessoais de clientes e usuários. As empresas precisam se conscientizar de que a proteção de dados não é apenas uma obrigação legal, mas também uma responsabilidade ética e moral, que pode afetar a imagem e a reputação da organização.

Portanto, é necessário continuar avançando na cultura de proteção de dados, educando e conscientizando a todos sobre a importância desse tema e incentivando a implementação de práticas de segurança e privacidade em todas as áreas da empresa. Só assim poderemos garantir a proteção adequada dos dados pessoais e a segurança dos clientes e usuários.

REFERÊNCIAS

ALLIANCE, National Cybersecurity. **Online Safety Basics**. 2022. Disponível em:< https://staysafeonline.org/resources/online-safety-basics/>. Acesso em 02 ago. 2023

BRASIL. Câmara dos Deputados. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 17 ago. 2022.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3ª Edição. Rio de Janeiro – RJ, Editora Forense, 2021.

CENTER, Pew Research. **How Americans think about privacy and the vulnerability of their personal data.** 2019. Disponível em: <https://www.pewresearch.org/internet/2019/11/15/how-americans-think-about-privacy-and-the-vulnerability-of-their-personal-data/ >. Acesso em 03 ago. 2023

CETIC, Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil [CETIC]. 2021. **Indicadores empresas, por práticas de segurança digital.** Disponível em:<https://data.cetic.br/explore/?pesquisa_id=4>. Acesso em 25 ago. 2022.

CHAGAS, Edigar Thiago de Oliveira. **Lei Geral de Proteção de Dados nas Organizações**. 1ª Edição. Orlando, FL, USA. . Ambra University Press, 2020.

DADOS, Autoridade Nacional de Proteção de. **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte**. 1ª Edição. Brasília-DF.

Editora: Venâncio, 2021. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>. Acesso em: 11 out. 2022.

DAVENPORT, Thomas. **Dados demais!: como desenvolver habilidades analíticas para resolver problemas complexos, reduzir riscos e decidir melhor**. 1ª Edição. Rio de Janeiro-RJ. Editora: Elsevier, 2014.

FÁVERO, Luiz. Paulo.; BELFIORE, Patrícia. **Manual de análise de dados**. 1ª Edição. Rio de Janeiro – RJ. Editora: LTC, 2022. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788595155602/epubcfi/6/8[%3Bvnd.vst.idref%3Dcopyright.xhtml]!/4>. Acesso em 22 de out. 2022.

FÁVERO, Luiz. Paulo.; BELFIORE, Patrícia. **Manual de análise de dados: estatística e modelagem multivariada com Excel**. 1ª Edição. Rio de Janeiro – RJ. Editora: SPSS® e Stata®, 2017. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788595155602/epubcfi/6/54[%3Bvnd.vst.idref%3Dchapter11.xhtml]!/4/2/2/100/4%4065:71>. Acesso em 12 de jan. 2023.

GUERREIRO, Ruth Maria.; TEIXEIRA, Tarcísio. 2022. **Lei Geral de Proteção de Dados Pessoais: comentada artigo por artigo**. 4ª Edição. São Paulo - SP. Editora: SaraivaJur, 2022.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. **"Foundations of Information Security: based on ISO 27001 and 27002.** Tradução: Alan de Sá. 3ª Edição. W 's-Hertogenbosch,The Netherlands. Editora: Van Haren Publishing, 2015.

LABS, Arkose. **Fraud & Abuse Report Q2 2020**. Disponível em: <https://www.arkoselabs.com/wp-content/uploads/Fraud-Report-Q2-2020.pdf>. Acesso em: 14 jun. 2022.

LIMA, Ana Paula Moraes Canto de.; **LGPD aplicada**. 1ª Edição. São Paulo - SP. Editora: Atlas, 2021.

LIMA, Cintia Rosa Pereira de. **ANPD e LGPD : desafios e perspectivas**. 1ª Edição. São Paulo – SP. Editora: Almedina, 2021.

MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**. Editora: Arquipélago Editorial LTDA. Porto Alegre – RS. 2020

PINHEIRO, Patrícia Peck. **Direito digital.** 7ª Edição. São Paulo - SP. Editora: Saraiva Educação, 2021. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555598438/epubcfi/6/4[%3Bvnd.vst.idref%3Dcopyright.html]!/4/10/2>. Acesso em: 15 out. 2022

PINHEIRO, Patricia Peck. **Proteção de dados pessoais:** comentários à Lei nº 13.709/2018 (LGPD). 2ª Edição. São Paulo -SP. Editora: Saraiva Educação, 2020.
São Paulo -SP.

PINHEIRO, Patricia Peck.; SLEIMAN, Cristina. **Segurança digital: proteção de dados nas empresas**. 1ª Edição. São Paulo -SP. Atlas, 2021.

POHLMANN, Sérgio. **Entendendo e Implementando a Lei Geral de Proteção de Dados nas empresas**. 2ª Edição. Rio de Janeiro – RJ. Editora: Verbis livros e leitura, 2021.

RUARO, Regina Linden; COELHO, Glitz; PANFOLFO, Gabriela. **Panorama geral da lei geral de proteção de dados pessoais no brasil e a inspiração no regulamento geral de proteção de dados pessoais europeu**. Revista de Estudos e Pesquisas Avançadas do Terceiro Setor, v. 6, n. 2 JUL/DEZ, p. 340- 356, 2020.

SINCLAIR, Bruce. **IOT: como usar a Internet das Coisas para alavancar seus negócios.** 1ª Edição. São Paulo - SP. Autêntica Business, 2018.

TEIXEIRA, Tarcísio. **Direito Digital e Processo Eletrônico**. 6ª Edição. São Paulo – SP. Editora: SaraivaJur, 2022.

TERADA, Routo. **Segurança de dados: criptografia em redes de computador**. 2ª Edição. São Paulo - SP. Editora: Blucher, 2008.

VÉLIZ, Carissa. **Privacidade é poder: por que e como você deveria retomar o controle de seus dados**. Tradução Samuel Oliveira; Ricardo Campos (prefácio). 1ª edição. São Paulo – SP. Editora Contracorrente, 2021.