



BUSINESS INTELLIGENCE E O DIREITO À PRIVACIDADE: APLICABILIDADE DA SEGURANÇA DA INFORMAÇÃO NAS RELAÇÕES DE CONSUMO

Submetido em: 30-08-2024
Publicado em: 18-10-2024

Jorge Fabricio dos Santos

Doutor, UFPA
Professor (IESP;EGPA; FAAM; DETRAN; EAP)
✉ fabricio06@yahoo.com.br

Cláudio Fernando de Souza Santos Junior

Mestre, UNAMA
Assessor Jurídico e advogado
✉ drelaudiosantos@hotmail.com

Roberto Magno Reis Netto

Doutor em Geografia, UFPA
Professor (IESP;EGPA)
✉ bob_reis_ufpa@yahoo.com.br

RESUMO: O uso do *Business Intelligence* (Inteligência empresarial) pelas organizações privadas carece de informações sobre o mercado para ofertar bens e serviços que atendam às suas demandas, utilizando-se de dados pessoais de seus consumidores, o que pode acarretar riscos à Segurança da Informação e a privacidade de seus clientes. Desta maneira, este artigo tem por finalidade demonstrar as normas jurídicas, técnicas e teóricas que apoiem a aplicação do *Business Intelligence* e Segurança da Informação no gerenciamento de informações pessoais de consumidores em instituições comerciais privadas. Foi adotada uma pesquisa aplicada, qualitativa, de cunho exploratório e descritiva, com uso de dados documentais e bibliográficos, com tratamento pela técnica de Análise para a apresentação dos resultados. Os resultados principais evidenciam que a prática do *Business Intelligence* requer a aplicação da metodologia da segurança da informação sobre os dados pessoais dos consumidores, a fim de protegê-los e atender aos requisitos constitucionais do Direito à Privacidade, pois há riscos de comercialização ilícita desses dados privados, bem com vazamentos para uso ilegítimo, podendo tais organizações serem responsabilizadas civilmente. Assim, propõem-se a adoção de procedimentos de segurança da informação, modificação dos sistemas das organizações para proteger esses dados, além da constante ciência dos consumidores para autorizações do uso de seus dados, além de novas pesquisas sobre o tema apresentado.

Palavras-chave: Inteligência empresarial; Dados pessoais; Consumidores; Riscos.

BUSINESS INTELLIGENCE AND THE RIGHT TO PRIVACY: APPLICABILITY OF INFORMATION SECURITY IN CONSUMER RELATIONS

ABSTRACT: The use of Business Intelligence by private organizations requires information about the market to offer goods and services that meet their demands, using personal data of their consumers, which can lead to risks to Information Security and the privacy of their customers. Thus, this article aims to demonstrate the legal, technical and theoretical standards that support the application of Business Intelligence and Information Security in the management of personal information of consumers in private commercial institutions. An applied, qualitative, exploratory and descriptive research was adopted, using documentary and bibliographic data, with treatment by the Analysis technique for the presentation of the results. The main results show that the practice of Business Intelligence requires the application of the information security methodology on the personal data of consumers, in order to protect them and meet the constitutional requirements of the Right to Privacy, as there are risks of illicit commercialization of this private data, as well as leaks for illegitimate use, and such organizations may be held civilly liable. Therefore, it is proposed to adopt information security procedures, modify organizations' systems to protect this data, in addition to constant awareness of consumers to authorize the use of their data, in addition to new research on the topic presented.

Keywords: Business intelligence; Personal data; Consumers; Risks.

1 INTRODUÇÃO

A relação de consumo não mais se resume à simples entrega de um bem e/ou ao fornecimento de um serviço por uma empresa privada, em busca da contrapartida financeira por parte do cliente (consumidor), seja em instituições no mundo físico ou no meio virtual. A atualidade jurídica requer que aquelas apliquem metodologias que venham a promover o direito constitucional à privacidade destes consumidores, sob diversas perspectivas.

Ocorre que, no meio virtual, é comum ter registros de incidentes de segurança da informação, que a ABNT (2005) define como “[...] um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade

de comprometer as operações do negócio e ameaçar a segurança da informação” (ABNT, 2005, p.2), de modo que esses problemas, em muitas ocasiões, fatalmente terão efeitos destrutivos quanto à privacidade das pessoas.

De acordo com o relatório atualizado de indicadores de incidentes de segurança da informação, do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), até o mês de agosto de 2024, foram notificados 249.048 registros, sendo que, no ano de 2023, foram registrados 621.537 incidentes em todo o Brasil (Brasil, 2024). Os números colocaram o Brasil como o líder de um *ranking* de 10 (dez) países que mais sofreram de incidente do tipo varredura e tentativa de ataque em sistemas de informação (com endereço de IP), no período de janeiro a julho de 2024, com 36,4% das notificações. A lista também apresenta os Estados Unidos (13,61%), China (12,73%) e Rússia (2,43%), sendo que, quanto ao incidente de *Scan*⁵², naquele mesmo período, o Brasil tem o maior percentual de registros (88,28%) com relação aos demais, podendo se afirmar o mesmo quanto às fraudes⁵³ (6,03%).

Assim, com esses dados alarmantes sobre a segurança da informação e a privacidade em risco, essa pesquisa definiu sua problemática: Em que medida as ferramentas de Segurança da Informação devem ser utilizadas pelas empresas privadas em seus bancos de dados para proteção de informações privadas de seus clientes, na prática de Inteligência empresarial, conforme a legislação em vigor e as pesquisas recentes? Ao passo, se estabeleceu como objetivo geral: demonstrar as normas jurídicas, técnicas e teóricas que apóiam a aplicação do *Business Intelligence* e Segurança da Informação, no gerenciamento de informações pessoais de consumidores, em instituições comerciais privadas.

E como meio direcionador do objetivo geral, foram estruturados os objetivos específicos: a) Apresentar o embasamento jurídico e doutrinário a respeito da segurança da informação e relações de consumo no Brasil; b) Apresentar metodologia Business Intelligence

⁵² “**Scan**: engloba além de notificações de varreduras em redes de computadores (*scans*), notificações envolvendo força bruta de senhas, tentativas mal sucedidas de explorar vulnerabilidades e outros ataques sem sucesso contra serviços de rede disponibilizados publicamente na Internet.” (Brasil, 2024).

⁵³ “**Fraude**: engloba as notificações de tentativas de fraude, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem, que pode ou não ser financeira. O uso da palavra fraude é feito segundo Houaiss, que a define como “qualquer ato arditoso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro”. Esta categoria, por sua vez, é dividida nas seguintes sub-categorias: *Phishing*: notificações de casos de páginas falsas, tanto com intuito de obter vantagem financeira direta (envolvendo bancos, cartões de crédito, meios de pagamento e *sites* de comércio eletrônico), quanto aquelas em geral envolvendo serviços de *webmail*, acessos remotos corporativos, credenciais de serviços de nuvem, entre outros. *Malware*: notificações sobre códigos maliciosos utilizados para furtar informações e credenciais.” (Brasil, 2024).

nas empresa privadas, conforme a bibliografia especializada; c) Descrever normatização legal acerca do direito à privacidade e à proteção de dados nas diversas instituições; d) Descrever a problemática da proteção de dados em acervos de informações virtuais de empresas privadas.

Este artigo científico justificou-se, primeiramente, por retratar uma discussão atual sobre o direito à privacidade, o qual os cidadãos-consumidores detém com relação aos seus dados pessoais que são coletados e utilizados por instituições privadas. Também revela sua importância num aspecto institucional, pois os conhecimentos apresentados poderão auxiliar gestores na condução de sistema de dados e executar protocolos que possibilitem a salvaguarda de dados de interesse pessoal de seus consumidores. Neste diapasão, compreende-se ainda a pertinência acadêmica, na medida em que, embora haja pesquisas publicadas quanto à proteção de dados de consumidores, é bastante escassa a produção científica no que tange ao uso da metodologia da segurança da informação em instituições de natureza privada que forneça bens e serviços.

A problemática recebeu as seguintes questões norteadoras: Como se apresentam os fundamentos normativos e bibliográficos com relação à segurança da informação e relações de consumo no Brasil? Como é aplicada a Inteligência empresarial, mediante a produção acadêmica? Quais as normas jurídicas relativas ao direito à privacidade e à proteção de dados nas diversas instituições? De que forma se observa a problemática da proteção de dados em agrupamentos de informações pelo meio virtual nas organizações privadas?

Neste artigo, aplicou-se, quanto aos procedimentos técnicos, uma pesquisa bibliográfica e documental, com dados coletados, respectivamente, em obras científicas publicadas e em normas jurídicas em vigência, referentes ao tema em estudo (GIL, 2008). No que tange à finalidade do estudo, foi realizada uma pesquisa aplicada, haja vista, objetivar uma análise de um problema jurídico e social comum no Brasil, para propor possíveis formas de resolução (Prodanov; Freitas, 2013).

Quanto à forma de abordagem, a pesquisa deu-se de maneira qualitativo, uma vez que as fontes de dados se consolidaram em textos de obras doutrinárias e normas jurídicas acerca do direito fundamental à privacidade e formas de proteção de dados pessoais, bem como a metodologia de gestão de dados corporativos e as relações de consumo (Prodanov; Freitas, 2013). Ainda neste artigo, quanto aos objetivos do estudo acadêmico, foram realizadas pesquisa tanto exploratória quanto descritiva, na medida em que inicialmente foi apresentado

tema de forma geral e em seguida descrição deste correlacionando os seus elementos de forma meticulosa (Gil, 2008).

Como *locus* de pesquisa foi estabelecido obras e normas publicadas no Brasil, e como fontes de dados de produção científica os diretórios de busca da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES e *Scientific Eletronic Library Online - SciELO*, e os normativos nos *websites* institucionais dos órgãos estatais, de modo que sua coleta ocorreu de forma remota, com acesso eletrônico dessas bases de dados. Após as coletas dos dados, foi aplicada a técnica de Análise de Conteúdo para processar os elementos textuais e extrair as informações de maior relevância para a pesquisa e demonstração sistemática dos resultados (Bardin, 2016).

2 RELAÇÕES DE CONSUMO

O ato jurídico de consumir produtos e serviços está no cerne da relação no ambiente capitalista, sendo natural que haja desproporcionalidade entre as partes envolvidas nesse ambiente comercial (Monteiro, 2020), que diante dessa realidade, o Estado passou a regulá-la, a fim de proteger o polo mais frágil, no caso o consumidor (Andrade, 2017; Verbicaro, 2018), sendo editada várias normas jurídicas, dentre estas a Lei Nº 8.078/1990 (Código de Defesa do Consumidor - CDC) que entrou em vigência em 1990 (Brasil, 1990).

Neste sentido, há várias definições referentes à relação de consumo, que de acordo com De Sousa (2021):

[...] se traduz em toda relação jurídica que existe entre uma pessoa, que deseja adquirir um bem ou prestação de um serviço, e outra que corresponde a este anseio. Desse modo, para que uma relação de consumo seja constituída, é necessária a integração de dois elementos essenciais, quais sejam: o consumidor e fornecedor (De Sousa, 2021, p. 6).

No texto acima tem-se que, para haver a relação consumerista, deve haver pelo menos o fornecedor do bem ou serviço e a pessoa que tenha interesse em obtê-los, não sendo obrigatório que ocorra a consumação do ato jurídico, como dispõe o Art. 29 da Lei Nº 8.078/1990 (Brasil, 1990), criando-se, portanto, uma relação de obrigações e direitos, mesmo antes de ocorrer a aquisição a título oneroso - podendo esta, inclusive, nem ser de fato efetivada (Scharf *et al.*, 2017).

3 DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS

Dentre vários direitos fundamentais que integram a dignidade da pessoa humana em toda sua completude, destaca-se o da privacidade (Cancelier, 2017), sendo que a Constituição Federal de 1988 dispõe, no seu art. 5º, inciso X:

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; (Brasil, 1988).

Cancelier (2017) discorre que o ordenamento jurídico brasileiro prevê direito à vida privada, além do direito à privacidade, os quais podem tanto serem sinônimos, quanto complementares, pois ambos estão relacionados à proteção da vida íntima da pessoa (Barreto Junior; Sampaio; Gallinaro, 2018), sendo o limite entre a vida pública e privada determinada pelo próprio indivíduo.

Embora Peixoto e Ehrhardt Júnior (2020) compreendam que o termo “privacidade” possua inúmeros significados variando em tempo e espaço geográfico (Brandeis; Warren, 2024; Lima, 2016), ponderando três dimensões complementares, quais sejam: decisional, informacional e espacial, nesta pesquisa analisa-se a interpretação informacional, os quais descrevem como dimensão relativa à proteção da informação.

No que se refere à proteção de dados pessoais, tal direito fundamental foi assegurado no art. 5º, inciso X da Constituição Federal de 1988 e no inciso LXXIX, disposto como “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” (Brasil, 1988).

A proteção de dados ganhou suporte normativo mais direto a partir da Lei Nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) que explicitou conceitos, métodos de proteção e controle, sujeitos responsáveis e outras regulamentações que buscam efetivar o direito fundamental (Carvalho; Pedrini, 2019).

4 SEGURANÇA DA INFORMAÇÃO

O termo Segurança da Informação, de acordo com a ABNT (2005), designa a “proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio” (ABNT, p.10, 2005), sendo que fica evidenciado que a segurança da informação trata-se de medidas que a organização desenvolve, a fim de proteger os dados com uso desde protocolos, passando por sistemas de informações, normas de gerenciamento de dados e *hardwares*.

Gonçalves (2015) destaca que no âmbito privado, a segurança da informação tem por finalidade, além da proteção de informações, que a organização alcance seus objetivos estratégicos e de negócio, além de diminuir o risco da própria atividade da instituição (Santos, 2014).

A Segurança da Informação, de acordo com os autores, se resumiria nas qualidades da informação, como a confidencialidade, integridade e disponibilidade (Nonato; Aganette, 2021), que foram estabelecidas pela norma técnica da Associação Brasileira de Normas Técnicas - ABNT (2005)⁵⁴.

Em termos legais, a LGPD (Brasil, 2018) destaca em seu art. 6º que o tratamento de dados pessoais:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; (Brasil, 2018).

Assim, a LGPD relaciona a segurança com processos e procedimentos determinados a fazer com que a organização proteja seus colaboradores internos e usuários de quaisquer riscos, de forma intencional ou acidental, de modo a promover o direito à privacidade e à intimidade.

Nardelli (2021) destaca que a LGPD é a norma que possui o embasamento legal que expressa todo o processo organizacional a ser empregado para prevenção de ataques aos sistemas de dados institucionais que violem informações pessoais (Brasil, 2018).

⁵⁴ “a) confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso; b) integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento; c) disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário” (ABNT, 2005).

Anteriormente, pela Lei Nº 12.965/2014 (Brasil, 2014), denominado Marco Civil da Internet, o legislador previu meios de controle de dados registros por meio eletrônico em rede, conforme o art. 10 dados pessoais e de acesso, além de conteúdos dessas comunicações em sítios eletrônicos e demais sistemas de informação. No seu art. 11, a norma legal também estabeleceu atribuições às empresas de comunicações (chamados provedores de *internet*) para proteção da privacidade, dos dados pessoais e sigilos das comunicações, com a devida responsabilização pelo descumprimento (Brasil, 2014).

Araújo Neto e Aguiar (2024) asseveram que atualmente a gama de dados que transitam em ambientes virtuais requer processos de segurança da informação para tratamento e controle, a fim de evitar ações ilícitas como invasões em sistemas de informações ou ataques para desabilitar e inutilizar tais acervos de dados.

Com a evolução da Tecnologia da Informação, meios de comunicação instantâneas, como as redes sociais, aumentaram as interações entre as pessoas ao mesmo tempo que os riscos advindos desses meios cresceram de forma exponencial (Lima, 2016; Veiga, 2020).

Passo (2017) destaca que o risco advém de utilização de recursos tecnológicos informacionais, os quais permeiam a convivência no mundo moderno, sendo utilizados para diversão, trabalho, estudo, transações bancárias, com registro de dados pessoais e o próprio histórico de acesso aos ambientes virtuais, integrantes de acervos de instituições privadas, constituindo em inovadora forma de observar o direito à privacidade.

A ABNT discorre que a segurança da informação tempo objetivo propiciar a proteção da informação nas organizações, de modo que estas tenham confidencialidade, integridade e disponibilidade, além da autenticidade, responsabilidade, confiabilidade e não repúdio (ABNT, 2005).

5 BUSINESS INTELLIGENCE -BI

As organizações empresariais, para manutenção de suas atividades e obtenção de lucros, empregam ferramentas que favorecem sua permanência no mercado, atendendo seus clientes de forma satisfatória e, para tal, estas têm necessidade de conhecer o ambiente em que atuam, bem como seus clientes, sendo utilizada, dentre vários instrumentos, a *Business Intelligence (BI)*.

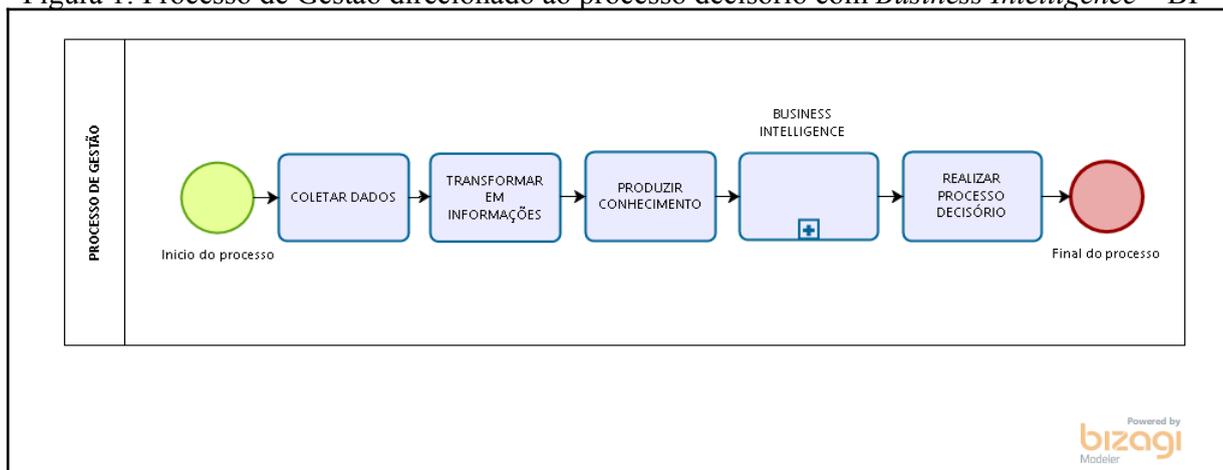
Angeloni e Reis (2006) comentam que:

Business Intelligence está ligado a Inteligência de Negócios ou Inteligência Empresarial, compõe-se de um conjunto de metodologias de gestão implementadas através de ferramentas de *software*, cuja função é proporcionar ganhos nos processos decisórios gerenciais e da alta administração nas organizações, baseada na capacidade analítica das ferramentas que integram em um só lugar todas as informações necessárias ao processo decisório (Angeloni; Reis, 2006, p. 3).

Desta definição de Angeloni e Reis (2006) infere-se que o *BI* realiza operações em dados contidos em bancos de dados empresariais, como o único objetivo de proporcionar base adequada para a gestão oriente suas ações empresariais mediante decisões estratégicas⁵⁵, o mesmo entendimento de Antonelli (2009).

Assim, concebe-se o *Business Intelligence* conforme um processo organizacional, baseado na compreensão de Antonelli (2009), demonstrado na Figura 1:

Figura 1: Processo de Gestão direcionado ao processo decisório com *Business Intelligence* – BI



Fonte: Autores adaptado de Angeloni e Reis (2006) e Antonelli (2009).

Percebe-se que o processo de gestão se inicia com a coleta de dados pela organização, que pode ocorrer com buscas dos setores ou mesmo acesso de consumidores (ou virtuais consumidores) em ambientes virtuais, sendo seguido pela tarefa de transformação desses elementos genéricos em informações, e após na produção de conhecimentos os quais tem valor para a instituição. Posteriormente, com o conhecimento elaborados, os sistemas de BI entrarão em cena com regras de negócio (área de atuação da organização) para requintar os conhecimentos a fim de serem utilizados pela gestão em processos decisórios que beneficiem a empresa (Petrilik; Gonzales; Auqui, 2023).

⁵⁵ “Decisão: é o processo pelo qual são escolhidas algumas ou apenas uma entre muitas alternativas para as ações a serem realizadas, esta escolha deve estar embasada pelo maior número possível de informações e conhecimento para que a decisão escolhida seja a melhor dentre as disponíveis” (Antonelli, 2009, p. 19).

É com essa concepção que Strassburg, Garcia e Garcia (2012) definem *Business Intelligence* como:

[...] ferramenta que auxilia as empresas na tomada de decisões estratégicas. Seu processo inicia-se por meio da coleta, organização e compartilhamento das informações. Após, esses dados são transformados em informações qualitativas que proporcionam o suporte necessário ao gestor dos negócios (Strassburg; Garcia; Garcia, 2012, p.19).

Mauri (2021) complementa dados de Angeloni e Reis (2006) e Antonelli (2009) ao assinalar que os dados aplicados no processo de Business Intelligence em regra são colhidos sistematicamente em fontes diversas, além dos fornecidos por colaboradores e consumidores de seus produtos e serviços.

Strassburg, Garcia e Garcia (2012) acrescentam que o *BI* tem como matéria prima a informação, que é obtida de fonte diversificada (inclusive dos registros de acesso de seus clientes), que após transformadas em conhecimentos são aplicados pela alta gestão no seu processo decisório. Essa atividade do *BI* para ser efetiva deve estar de posse de informações precisas, oportunas e tempestivas, pois a não observância destas características intrínsecas podem gerar conhecimentos inadequados e, por conseguintes, decisões que prejudiquem a manutenção da empresa como perdas de seus ativos (Angeloni; Reis, 2006; Zabaleta; Luna, 2022).

Barbieri (2011) informa que a *Business Intelligence* se caracteriza como uma metodologia de organização de dados (modelagem) em banco de dados das organizações privadas, que detém as informações de registros (como histórico de acesso e alterações), que com meios tecnológicos (*softwares*, algoritmos) possui a capacidade de análise de padrões imprescindíveis para as atividades empresariais.

Com menciona Barbieri (2011), a Tecnologia da Informação é crucial para o sucesso de BI nas organizações empresariais, de modo que Debotoli e Brignole (2024) afirma que se inserem no Business Intelligence, além de conjunto de algoritmos e ferramentas de análise de dados, instrumentos e técnicas da Estatísticas e outros elementos tecnológicos, como a mineração de dados e modelagem matemática.

6 PROTEÇÃO DE DADOS EM ESTABELECIMENTOS PRIVADOS

O Código de Defesa do Consumidor – CDC (Lei N° 8.078/1990) estabelece que os cadastros de dados dos consumidores devem ser protegidos (Brasil, 1990), de modo que estes

são considerados de caráter público (art. 43, §4º), ou seja, não são propriedade exclusivas das instituições que os criaram e os mantém, porém esta condição não autoriza que os dados sejam liberados para uso de quaisquer pessoas, uma vez que referem-se, em muitos cadastros, em que há informações que afetam a privacidade dos consumidores, requerendo determinados cuidados.

De acordo com Pinto e Soares (2021), embora a legislação consumerista tenha previsto a obrigatoriedade, os fornecedores de serviços e bens não cumprem atividades de segurança da informação em seus bancos de dados de clientes, quanto aos dados pessoais e informações de consumo.

Neste sentido, Goulart (2012) destaca que o requisito de confidencialidade das informações disponibilizada pelo consumidor obriga que esta deve ser observada desde a coleta nos acervos do fornecedor até a transferência de dados para quaisquer usos lícitos.

A ABNT (2005) em sua norma “ABNT NBR ISSO/IEC 27002:2005. Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação” tem como uma de suas premissas a proteção de dados pessoais e outros da organização, como por exemplo os de consumo, dados financeiros e outros.

Considerando os números elevados de incidentes de segurança da informação, cabe à organização utilizar de técnicas e instrumentos de segurança da informação para debelar tais situações, uma vez que pelas ações de pessoas com interesses escusos, que utilizam a rede mundial de computadores que acessam os sítios eletrônicos das instituições comerciais, estes, detentores de uma vasta gama de dados pessoais de seus usuários-consumidores, inclusive dados financeiros decorrentes de transações bancárias (Soares, 2023).

Garcia (2015) afirma que dentre vários direitos do consumidor, o relativo à informação caracteriza-se como direito fundamental, pois na sociedade atual mediatizada por sistemas de comunicações tecnológicas instantâneas, a prerrogativa de proteção das informações pessoais e acesso a dados de consumo passaram a ter um interesse de vários atores sociais, além do próprio consumidor (Follone; Simão Filho, 2020).

No que concerne às obrigações das empresas que operam no comércio eletrônico (*e-commerce*), Pereira (2022) aponta a responsabilidade civil extracontratual para indenizar os consumidores que tenham sido violados no direito à privacidade de seus dados por omissão destas organizações.

A realidade, como demonstram Rocha, Fontes e Machado (2023), é de que as empresas brasileiras não estão de acordo com as premissas da LGPD no que tange a segurança da informação, haja vista, a escassez de pessoas qualificadas no mercado, prejudicando a gestão de dados no ambiente físico e virtual.

Para atendimento das premissas de segurança da informação e atendimento da legislação, as empresas deverão coletar e armazenar tais dados, sempre mantendo os requisitos de confidencialidade, integridade e disponibilidade, sempre com enfoque à proteção de privacidade, por isso deve possuir mecanismos de proteção contra incidentes de segurança da informação, pois assim pode ser prevenido que informações das bases de dados da organização não venha a ser obtidas por pessoas com objetivos ilícitos, que, de posse destes dados, podem cometer ilícitos financeiros ou morais contra os consumidores proprietários das informações (Neves *et al.*, 2021; Dias; Brasil; Ferreira, 2023).

Essas atividades quanto ao tratamento das informações, requeridas pela LGPD, como expressam Duarte, Domeniconi Junior e Eboli (2022) refere-se a mapeamento, classificação da informação, além da definição da finalidade destas, bem como estabelecimento de operadores, do ciclo de vida da informação, e estrutura de controle de conformidade, a fim de possibilitar que as informações dos consumidores estejam de acordo com os requisitos citados anteriormente e o direito à privacidade dos usuários da organização (Follone; Simão Filho, 2020). Neste sentido, a estruturação de adequados Sistemas de Informações (SI) constitui-se como pressuposto essencial para o atingimento das metas organizacionais e jurídicas da instituição (Nascimento Junior; Lobato, 2022).

Dias, Brasil e Ferreira (2023) aponta que a revolução informação do final do século XX e início do atual aumentou o poder controle das grandes corporações da área de TI, sendo que pelo volume de dados coletados em acessos ou em transações comerciais, aumentou o lucro dessas empresas privadas ao mesmo tempo que o risco cresceu no mesmo patamar, já que informações são ativos que possuem valor no mercado, principalmente dados de natureza pessoal como número de documentos (RG, CPF), condições financeiras, localização geográfica e interesses de consumo (Follone; Simão Filho, 2020), nem sempre com a autorização do consumidor (Bergstein; Aragão; Câmara, 2022), por esse motivo a adoção da metodologia de segurança da informação na LGPD, na medida que na relação jurídica entre o fornecedor e o consumidor, este último sempre estará em condição de vulnerabilidade (Nascimento, 2015).

Verifica-se determinadas práticas institucionais que com consciência ou de forma não esperada, podem acarretar lesão ao direito à privacidade relativo aos dados pessoais adquiridos pelas organizações empresariais, tais como a comercialização e o vazamento de dados.

No que concerne ao vazamento de dados de dados, Santos e Freitas (2024) informa que as organizações não têm domínio total dos dados que impeçam que os dados pessoais sejam acessados e disponibilizados por pessoas não autorizadas, tendo em vista a condição do cibernético a que estão inseridas, de modo que este vazamento pode ocorrer tanto por erros técnicos da própria empresa ou por furto de terceiros. Esse problema vem atingindo o setor público, porém muitas vezes ocorre que organizações privadas que prestam serviços terceirizado de tecnologia da informação sofrem esses incidentes em função das fragilidades técnicas de pessoas que manipulam esses dados pessoais (Galvão *et al.*, 2024).

Em complemento a essa realidade, Oliveira e Novais (2024) informa que as empresas devem implementar uma política de segurança da informação e treinamento de funcionários como medidas para atender a LGPD e tratar desses vazamentos de informações, uma vez que várias consequências podem surgir desse incidente, como roubo de identidade, fraudes financeiras e patologias mentais aos proprietários dos danos pessoais.

Verifica-se ainda a existência do dano moral no vazamento de dados quando este se efetive mesmo não havendo o uso dos dados pessoais em ações ilícitas, pois segundo a legislação civil brasileira informa que havendo o dano o direito de reparação deve ser aplicado a quem deu causa, sendo que o terceiro que destes dados obtido ilegalmente e os utiliza, também são passíveis de pagamento de valores referidos a dano causado, no enquadramento de dano moral e responsabilidade civil (Ferreira; Garcia, 2024). Isso se verifica nos casos de fraudes bancárias ou no acesso de *hackers* aos sistemas de informações de instituições financeira detentores dos dados pessoais de seus consumidores, neste último caso cabendo a responsabilidade subjetiva (Severiano; Gominho, 2021).

Outro exemplo de responsabilidade civil da empresa pelo vazamento de dados é o que se refere ao uso de inteligência artificial em utilização de comunicação de empresas, como o *ChatGPT*, e na realização de tarefas, pois há o armazenamento de dados de funcionários quanto ao acesso e respostas que os *softwares* fornecem, que podem ser acessadas indevidamente por pessoa não autorizados, vide as fraquezas da segurança da informação.

Esse problema mostra-se mais grave em virtude que até a presente data não há regulamentação da inteligência artificial no Brasil (Botton; Trevisol, 2023).

Referente ao uso indevido de dados e informações de usuários que estão em banco de dados de empresas, a LGPD veda tal prática irregular, considerando que o cidadão que tenha esse direito violado acessa ao Poder Judiciário e requeira a devida reparação pelo dano sofrido, pois o uso não autorizado de suas informações afronta ao direito à privacidade tutelador pelo texto constitucional (Leal, 2021).

Sobre comentários da Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (UE), Antunes (2021) discorre sobre a economia sobre a comercialização de dados de natureza diversa para a produção de produtos, porém assevera que a norma europeia considera violação de direitos pessoais o comércio de dados sobre as pessoas sem a devida autorização, haja vista, a inexistência de contrato prévio mantido entre a organização privada e o usuário do sistema.

Martínez, Damasceno e Macedo (2019) apresentam perspectivas sobre uso das informações na sociedade capitalista como produto a ser comercializado, com dados referentes aos comportamentos humanos em atividades de lazer, trabalho, sociabilidades, consumo, e outras atividades sociais. Os autores destacam essa economia informacional a que se dedicam empresas como *Google, Facebook, Twitter, Yahoo, Experience*, as chamadas *big techs*, com lucros exorbitantes, mediante fornecimento gratuito de serviços, mas com captação desses dados pessoais (Marcelino *et al.*, 2024).

7 CONSIDERAÇÕES FINAIS

Esta pesquisa científica objetivou verificar o uso da Segurança da Informação pelas empresas privadas quando do emprego da Inteligência empresarial em seus bancos de dados no que tange à proteção de informações privadas de seus clientes, mediante as normas jurídicas em vigor.

Para tal foi desenvolvida uma pesquisa bibliográfica e documental, sob a premissa de um estudo aplicado, sobre dados qualitativos, com viés exploratório e descritivo, para exame do conteúdo dos normativos e teóricos, para responder satisfatoriamente à pergunta problema, no que foi ratificada a conexão entre as práticas corporativas de inteligência quanto aos dados

peçoais de consumidores e o direito à privacidade permeada pela Segurança da Informação, de forma que os objetivos da pesquisas foram plenamente alcançados.

Verificou-se que nas relações de consumo, a posição da empresa, enquanto fornecedor de bens e serviços, para os consumidores (seus clientes), perpassa atualmente por uma relação jurídica que na atualidade é mediada por meios tecnológicos, mediante utilização de sítios eletrônicos na Internet, de modo que o no acesso à esses ambientes virtuais, o consumidor produz dados e informações, além daqueles relacionados às suas preferências de compra, mas também considerados dados de natureza privada, que estão protegidos pelo direito fundamental à privacidade, previsto na Constituição Federal de 1988, sendo que além dessa prática há o emprego da Inteligência Empresarial (*Business Intelligence*) para coleta dessas informações e outras, que podem afetar negativamente esse direito constitucional os consumidores.

O presente artigo apresentou essa realidade calcada em normas jurídicas internacionais e nacionais quanto a proteção de dados pessoais pela internet, concernente à metodologia *Business Intelligence* e sua relação com dados de consumidores, deixando evidente que a empresa privada, que coleta tais dados pessoais, pode estar sujeita à responsabilização civil, quando não emprega as técnicas de Segurança da Informação desde a aquisição até o emprego de tais dados.

A pesquisa também apontou que existe normas técnicas e jurídicas que descrevem adequadamente a forma de utilização da Segurança da Informação, e ainda apresenta as práticas que ofendem ao Direito à privacidade dos consumidores, como a comercialização irregular de dados pessoais sem autorização destes, bem como o vazamento de dados, sejam por acesso ilegítimo de pessoas externas (*hackers*), seja por falhas internas de pessoas ou de sistemas inadequados para o uso dessas informações.

Assim, esta pesquisa destaca que o emprego do *Business Intelligence*, ao mesmo tempo que propicia que a empresa privada se manter no mercado, pode também ser um meio, quando não observadas as premissas e ferramentas de Segurança da Informação, podem colaborar mesmo que de formas não proposital para ações ilícitas em dados pessoais de seus consumidores, afetando diretamente ao direito à privacidade.

Desta maneira, propõem-se que sejam construídos protocolos do uso do *Business Intelligence* nas empresas, seguindo as orientações da Segurança da Informação, ao mesmo tempo que os sistemas informacionais sejam adequados a esses pressupostos de segurança.

Sugere-se também que haja mecanismos de comunicação ao consumidor que acesse aos ambientes virtuais empresariais sobre a coleta de dados, sendo que este tenha conhecimento do uso de seus, para optar em aceitar ou não que a empresa os utilize, bem como que sejam estabelecidas normas jurídicas para regular a *Business Intelligence*. Sendo proposto, ao fim a produção de outras pesquisas nesta temática, com o fito de amadurecer a discussão no meio acadêmico.

REFERÊNCIAS

- ANDRADE, Gustavo Henrique Baptista. A boa-fé nas relações de consumo: Informação e defesa do contratante vulnerável nas situações de superendividamento. **Revista OAB/RJ - Edição Especial – Direito Civil**. Rio de Janeiro, Revista OAB/RJ, p. 1-26, 2018.
- ANGELONI, Maria T., REIS, Eduardo S. **Business Intelligence como Tecnologia de Suporte a Definição de estratégias para melhoria da qualidade do ensino**. In: Encontro da ANPAD, 2006, Salvador. XXX Encontro Nacional de Pós-Graduação em Administração, 2006, 2006. V. 1. p. 16 páginas.
- ANTONELLI, Ricardo Adriano. Conhecendo o Business Intelligence (BI): Uma ferramenta de Auxílio à Tomada de Decisão. **Revista TECAP - Tecnologia e Contabilidade em Pesquisa**, Pato Branco, n. 3, a. 3, v. 3, p. 79-85, 2009.
- ANTUNES, Henrique Sousa. Os dados: entre a proteção e a comercialização. p.43- 65. In: SEQUEIRA, Elsa Vaz de (Org.). **Católica talks: Direito e Tecnologia**. Universidade Católica Editora: Lisboa, 2021.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR ISSO/IEC 27002:2005. Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. São Paulo: ABNT, 2005.
- ARAÚJO NETO, Reinaldo Juvino de; AGUIAR, Janderson Jason Barbosa. Os impactos da Lei Geral de Proteção de Dados (LGPD) na segurança da informação: uma revisão da literatura. **Revista Gestão e Secretariado (GeSec)**, São Paulo, SP, v. 15, n. 2, p. 01-20, 2024.
- BARBIERI, Carlos. **BI – Business Intelligence: Modelagem e Tecnologia**. Rio de Janeiro, Axcel Books, 2001.
- BARDIN, Laurence. **Análise de Conteúdo**. Ed., Rev., Ampl. São Paulo: Edições 70 Brasil, 2016.
- BARRETO JUNIOR, Irineu Francisco; SAMPAIO, Vinícius Garcia Ribeiro; GALLINARO, Fábio. Marco civil da internet e o direito à privacidade na sociedade da informação. **Direito, Estado e Sociedade**. Rio de Janeiro, n.5, jan/jun, p. 114-133, 2018.

BERGSTEIN, Laís; ARAGÃO, Flávia Gama de Carvalho; CÂMARA, Maria Amália. Proteção de dados pessoais e as decisões automatizadas nas relações de consumo: os direitos à explicação e revisão. **Revista de Direito do Consumidor**. São Paulo, v. 140, Mar./Abr., p. 359-385, 2022.

BOTTON, Vitor Luís; TREVISOL, Lucas Kayser. Responsabilidade civil pela violação de dados pessoais por meio da inteligência artificial. **Revista UNITAS**. Itapiranga, n. 8, p. 136-152, 2023.

BRANDEIS, Louis D.; WARREN, Samuel D. O direito à privacidade. **Revista de Direito Civil Contemporâneo**. São Paulo, v. 38, a. 11, p. 391-417, jan./mar., 2024.

BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br. Estatísticas do CERT.BR. **Incidentes notificados ao CERT.br – Incidentes notificados voluntariamente ao CERT.br por CSIRTs, administradores e redes e usuários finais [atualização mensal]**. Disponível em:<<https://stats.cert.br/incidentes/#incidentes>>. Acesso em: 26 ago. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em:<https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 18 ago. 2024.

BRASIL. Lei Nº 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências**. Disponível em:<https://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm>. Acesso em: 19 ago. 2024.

BRASIL. Lei Nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 19 ago. 2024.

BRASIL. LEI Nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm>. Acesso em: 17 ago. 2024.

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência**. Florianópolis, n. 76, ago., p. 213-240, 2017.

CARVALHO, Gisele Primo; PEDRINI, Tainá Fernanda. Direito à privacidade na lei geral de proteção de dados pessoais. **Revista da ESMESC**. Florianópolis, v. 26, n. 32, p. 363-392, 2-19.

DEBORTOLI, Diego Oscar; BRIGNOLE, Néida Beatriz. Inteligencia empresarial para estimular el giro comercial en el microcentro de una ciudad de tamaño intermedio. **Región Científica**, v. 3, n. 1, p. 2024195-2024195, 2024.

DE SOUSA, José Franklin. **Relação de consumo e seus elementos**. Joinville: Clube de autores, 2021.

DIAS, Aurora de Nazaré Fernandes; BRASIL, Luiza Arruda Camara; FERREIRA, Vanessa Rocha. A utilização de tecnologias pelas *big techs* para obter vantagens desleais no mercado digital. **Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo**. Florianópolis, Encontro Virtual, v. 9, n. 1, Jan/Jun., p. 01 – 17, 2023.

DUARTE, Elton Pereira; DOMENICONI JUNIOR, Romeu; EBOLI, Daisy. **LGPD: medidas essenciais de segurança da informação**. In: II FatecSeg - Congresso de Segurança da Informação – 17 e 18 de novembro de 2022. Disponível em:<<https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/68/27>>. Acesso em: 25 ago. 2024.

FERREIRA, Lucia Maria Teixeira; GARCIA, Matheus. Responsabilidade civil por vazamento de dados pessoais: análise da decisão proferida no AREsp n. 2.130.619/SP. **Civilistica.com**. Rio de Janeiro. a. 13, n. 2, p. 1-32, 2024.

FOLLONE, Renata Aparecida; SIMÃO FILHO, Adalberto. **A conexão da LGPD e CDC: a proteção de dados pessoais nas relações consumeristas e a sua concretização como direito fundamental**. In: Anais do Congresso Brasileiro de Processo Coletivo e Cidadania. Ribeirão Preto, n. 8, out., p. 937-959, 2020.

GALVÃO, Heideivirlandia Leite; OLIVEIRA, Alyne Leite de; GINO, Bethsaida de Sá Barreto Diaz; VIANA, Hudson Josino; ARAÚJO, Francisco Gledison Lima; BENEVINUTO, Noélia Marques Silva; SILVA, Denis Leonardo Ferraz da. Incidentes de Segurança: Regulação e Prática de Vazamento de Dados Pessoais Frente à LGPD. **ID On Line Revista de Psicologia**. Cariri, v.18, n. 72, Jul., p. 179-197, 2024.

GARCIA, Leonardo de Medeiros. O princípio da informação na pós-modernidade: direito fundamental do consumidor para o equilíbrio nas relações de consumo. **Revista Direito UNIFACS – Debate Virtual**. Salvador, n. 176, p.1-19, fev, 2015.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4 ed. São Paulo: Atlas, 2008.

GONÇALVES, Edison Luiz. **Políticas de segurança da informação**. Rio de Janeiro: RNP/ESR, 2015.

GOULART, Guilherme Damasio. **Segurança da informação e a proteção contra a violação de dados pessoais: A confidencialidade no Direito do Consumidor**. 2012. 215 f. Dissertação (Mestrado em Direito). Programa de Pós-Graduação em Direito, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2012.

LEAL, José Geraldo Alves. A Lei Geral de Proteção de Dados e a banalização no uso de dados pessoais no meio empresarial. **Ponto de Vista Jurídico**. Caçador, v. 10, n.02, jul./Dez., p. 63-79, 2021.

LIMA, Luciano de Almeida. **O direito à privacidade nas redes sociais na internet**. 101 f. 2016. Dissertação (Mestrado em Direito). Universidade Regional do Noroeste do Estado do Rio Grande do Sul. Ijuí, 2016.

MARCELINO, Danielle Alves Correia; COSTA, Douglas da Silva; QUARESMA, Ênison Victor Pereira; PÚBLIO, Carlos Alberto Maciel. Comercialização de dados pessoais sob a óptica do ornamento jurídico brasileiro: uma análise do caso da empresa de serviços de assessoria S.A (SERASA Experian). *REVISTA Foco*. Curitiba, v.17, n. 5, e5267, p. 1024, 2024.

MARTÍNEZ, Gabriel Francisco Cevallos; DAMASCENO, Handherson Leylton Costa; MACEDO, Társo Roberto Lopes. Privacidade e redes digitais: a comercialização de dados no ciberespaço. *Revista e-Curriculum*. São Paulo, v.17, n.3, jul./set., p.1393-1398, 2019.

MAURI, Rigoberto David García. Inteligencia Empresarial. *Pedagogía Profesional*. Havana, 19, n. 2, abr./jun., p.1-10, 2021.

MONTEIRO, Marli. Compliance nas relações de consumo. *Revista JurisFIB*. Bauru, Edição Especial 15 anos Direito FIB, dez., p. 29-41, 2020.

NARDELLI, Cleber. Segurança da Informação e LGPD Aplicado no Desenvolvimento de Software. *In: Escola Regional de Engenharia de Software (ERES)*, 5., 2021, Evento Online. *Anais*. Porto Alegre: Sociedade Brasileira de Computação, 2021, p. 169-178.

NASCIMENTO, Carlo Bruno Lopes do. A problemática da informação imperfeita nas relações de consumo e a necessidade de proteção do vulnerável. *Revista Jurídica Luso-Brasileira - RJLB*. Lisboa, n. 2, a. 1, p. 381-408, 2015.

NASCIMENTO JUNIOR, Aldo Evan Sousa do; LOBATO, Vinícius Edevandro da Silva. **Os princípios de tratamento de dados da Lei Geral de Proteção na Ótica de Sistemas de Informação**. 56f. 2022. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação). Universidade Federal Rural da Amazônia. Belém, 2022.

NEVES, Denise Lemes Fernandes; PAVANI, Guilherme Cintra; SALES, Rafael Marcos; LOPES, Tatiana Schmitz de Almeida. A segurança da informação de encontro às conformidades da LGPD. *Revista Processando o Saber*. Praia Grande, v. 13, jun., p.186-198, 2021.

OLIVEIRA, Larissa de Jesus; NOVAIS, Thyara Gonçalves. Lei Geral de Proteção de Dados Pessoais: responsabilidade civil no vazamento de informações. *Revista Íbero-Americana de Humanidades, Ciência e Educação*. São Paulo, v. 10, n.05, mai., p. 1614-1631, 2024.

PASSOS, Bruno Ricardo dos Santos. O direito à privacidade e a proteção aos dados pessoais na sociedade da informação: uma abordagem acerca de um novo direito fundamental. 102 f. 2017. Dissertação (Mestrado em Direito Público). Faculdade de Direito – Universidade Federal da Bahia. Salvador, 2017.

PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias. **Revista Jurídica Luso-Brasileira - RJLB**. Lisboa, n. 2, a. 6, p. 389-418, 2020.

PEREIRA, Fabiana de Almeida. E-commerce e proteção de dados pessoais: análise jurídico-legal sobre os fundamentos da responsabilidade. p. 186-213. In: BARRETO JUNIOR, Irineu Francisco; WALDMAN, Ricardo Libel (Orgs.). **Direitos humanos, ética e democracia na sociedade da informação III [livro eletrônico]: discurso de ódio na sociedade em rede**. 1. Ed. São Paulo: Ed. Dos Autores, 2022.

PETRLIK, Ivan; GONZALES, Pedro Lezama; AUQUI, José Antonio Ogosi. Inteligencia empresarial para mejorar la gestión del gasto en universidades públicas. **Revista Venezolana de Gerencia: RVG**. Maracaibo, v. 28, n. 103, jul./set., p. 1344-1358, 2023.

PINTO, Laryssa Carolyne Oliveira; SOARES, Douglas Verbicaro. Lei Geral de Proteção dos Dados Pessoais: análise acerca da proteção de dados do consumidor à luz da lei N. 13709/2018. **Revista Amor Mundi**. Santo Ângelo, v. 2, n. 6, p. 7-27, jun. 2021.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar. **Metodologia do trabalho científico** [recurso eletrônico]: métodos e técnicas da pesquisa e do trabalho acadêmico. 2ª ed. Novo Hamburgo: Feevale, 2013.

ROCHA, Roger Luz da; FONTES, Selma Velozo; MACHADO, Thiago Fontes. A segurança da informação nas organizações: um estudo sobre o impacto da Lei Geral de Proteção de Dados Pessoais na gestão. **RECH – Revista Ensino de Ciências e Humanidade – Cidadania, Diversidade e Bem estar**. Humaitá, v. VII, n. 2, jul/dez, p. 463-483, 2023.

SANTOS, Eurialle de Souza Rosa. Segurança da Informação. p. 76-86. In: GONÇALVES, Wilson José (Org.). **Termos Técnicos Fundamentais – teoria e prática**. Campo Grande: UFMS, 2014.

SANTOS, Ítalo Kelson Pereira dos; FREITAS, Gisela Carvalho. Vazamento de dados pessoais em tempos de informação instantânea. **Revista Íbero-Americana de Humanidades, Ciência e Educação**. São Paulo, v. 10, n.06, jun., p. 488-504, 2024.

SCHARF, Edson Roberto; DIAS, Feliciano Alcides; ZUCCO, Marcio Luiz; SAUT, Roberto Diniz. compro, logo existo ou por que uma disciplina envolvendo o comportamento do consumidor é basilar para o curso de Direito? **Visão**. Caçador, v. 6, n. 2, jul./dez., p. 101-117, 2017.

SEVERIANO, Gustavo Costa; GOMINHO, Leonardo Barreto Ferraz. Direito a privacidade na *Internet*: A Lei Geral de Proteção de Dados Pessoais. **Revista Jurídica Facesf**. Belém do São Francisco, v.3, n.2, p. 7-20, 2021.

SOARES, Miguel Ângelo Saragoça. **Manual prático para PME – Cibersegurança. Segurança da informação, privacidade e proteção de dados pessoais**. 223f. 2023. Dissertação (Mestrado em Cibersegurança e Informática Forense). Instituto Politécnico de Leiria. Leiria-Portugal, 2023.

STRASSBURG, Udo; GARCIA, Elias; GARCIA, Osmarina Pedro Garcia. **Um estudo da aplicabilidade do *business intelligence* em uma empresa do ramo da saúde.** In: I Congresso Brasileiro em Gestão de Negócios. XI Seminário do Centro de Ciências Sociais Aplicadas. XIII Jornada de Estudos Contábeis – Unioeste Cascavel – Ano 2012. Disponível em: <https://www.academia.edu/3854629/UM_ESTUDO_DA_APLICABILIDADE_DO_BUSINESS_INTELLIGENCE_EM_UMA_EMPRESA_DO_RAMO_DA_SA%C3%9ADE>. Acesso em: 24 ago. 2024.

VEIGA, Adélia Solange Pereira Gonçalves da. **Proteção de dados: o direito à privacidade na era digital.** 24f. 2020. Dissertação (Mestrado em Direito). Universidade Autónoma de Lisboa “Luís de Camões”. Lisboa, 2020.

VERBICARO, Dennis. A política nacional das relações de consumo como modelo de democracia deliberativa. **Revista Jurídica da Presidência.** Brasília, v. 19, n. 119, p. 534-559, Out. 2017/Jan./2018, 2018.

ZABALETA, Mercedes Elena Martínez; LUNA, Raúl Enrique Rodríguez. Inteligencia empresarial y su rol en la generación de valor en los procesos de negocios. **Tendencias,** v. 24, n. 1, p. 226-251, 2023.



BIOGRAFIA

Jorge Fabricio dos Santos

Mestre em Segurança Pública pelo Programa de Pós-Graduação em Segurança Pública da Universidade Federal do Pará (PPGSP/UFPA); Bacharel em Direito pela Faculdade Metropolitana da Amazônia (FAMAZ); Bacharel em Ciência de Defesa Social e Cidadania, pelo Instituto de Ensino de Segurança do Pará (IESP); Graduado em Tecnologia em Análise e Desenvolvimento de Sistemas, pelo Instituto Federal de Educação, Ciência e Tecnologia do Pará (IFPA); . É professor do Instituto de Ensino de Segurança Pública do Pará (IESP) no Curso de Formação de Oficiais PM, Curso de Habilitação de Oficiais (CHO), Curso de Adaptação de Oficiais (CADO), no Curso de Formação de Praças PM, Curso de Adaptação à Graduação de Sargentos (CGS) e Curso de Aperfeiçoamento de Sargentos (CAS). Tutor à distância dos cursos EaD do Ministério da Justiça, Tutor Presencial do Instituto Federal de Educação, Ciência e Tecnologia do Pará (IFPA), professor da Escola de Governança Pública do Pará (EGPA), professor da Faculdade da Amazônia (FAAM), do Departamento Estadual de Trânsito (DETRAN) e da Escola de Administração Penitenciária (EAP).

CONTATOS

 <http://lattes.cnpq.br/2274425533276987>

 fabrcio06@yahoo.com.br

Cláudio Fernando de Souza Santos Junior

Graduado em Direito pela Universidade da Amazônia. Pós-Graduado pela Universidade da Amazônia em Direito Material e Processual do Trabalho. Mestre em Direitos Fundamentais pela Universidade da Amazônia - UNAMA. Proprietário do escritório Claudio Santos - Consultoria Jurídica. Assessor Jurídico na Casa Militar da Governadoria do Estado. Advogado.

CONTATOS

 <http://lattes.cnpq.br/5902612590437360>

 drclaudiosantos@hotmail.com



BIOGRAFIA

Roberto Magno Reis Netto

Doutor em Direitos Humanos, pela Universidade Federal do Pará (2009). Mestre em Direito Penal, pela Universidade Federal do Pará (2002). Professor da Graduação e Pós-Graduação - Mestrado na Universidade da Amazônia (UNAMA). É Promotor de Justiça aposentado do Ministério Público do Estado do Pará. Tem experiência na área de Direito, com ênfase em Direito Penal, Processo Penal, Direitos Humanos e Criminologia.

CONTATOS

 <http://lattes.cnpq.br/5368010317556530>

 <https://orcid.org/0000-0002-5076-6149>

 bob_reis_ufpa@yahoo.com.br