A GARANTIA A PROTEÇÃO DO DIREITO DE PRIVACIDADE FRENTE AOS ALGORITMOS DE RECOMENDAÇÕES DE *E-COMMERCES* SOB A ÓTICA DA LGPD

Marcela Ferreira Guimarães[1]
Erika Tayer Lasmar[2]

Resumo: O presente artigo aborda as principais práticas recomendadas pela Lei Geral de Proteção de Dados (LGPD), para *e-commerces* que utilizam algoritmos de recomendação, visando proteger os direitos à privacidade e proteção de dados dos usuários, e abordando, também, como sugestão, formas para a implementação dessas principais práticas. A LGPD estabelece orientações sobre como os dados pessoais são coletados, armazenados, usados e compartilhados, com o objetivo de proteger os direitos dos indivíduos a quem esses dados pertencem, além de garantir a privacidade e a segurança das informações. No contexto do *e-commerce*, onde são utilizados algoritmos de recomendação que processam dados pessoais dos usuários, é fundamental adotar boas práticas de proteção de dados e privacidade para oferecer uma experiência segura tanto aos usuários quanto à empresa. O estudo consiste em pesquisa exploratória, com resultados qualitativos obtidos a partir de fontes secundárias, como artigos, sites, matérias publicadas em jornal estrangeiro e livros sobre o tema.

Palavras-chave: Lei Geral de Proteção de Dados, Práticas recomendadas *e-commerces, A*lgoritmos, Privacidade, Proteção de Dados

1INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018) estabelece regras claras para a coleta, o armazenamento, o uso e o compartilhamento de dados pessoais, visando proteger os direitos dos titulares desses dados e garantir a privacidade e a segurança das informações.

A LGPD (BRASIL, 2018) é extremamente importante, por diversos motivos, mas em principal, para o presente artigo, quando os algoritmos de recomendação são utilizados por *e-commerces*, pois estão sendo processados os dados pessoais dos usuários, e ao utilizarem e processarem esses dados surgem as obrigações, que são impostas pela Lei.

Portanto, adotar boas práticas de proteção de dados pessoais e ao direito à privacidade é fundamental para que as empresas de *e-commerce* possam oferecer uma experiência segura e confiável para os usuários. O presente artigo tem como foco principal abordar as práticas recomendadas, de acordo com a LGPD (BRASIL, 2018), a *e-commerces* que utilizam algoritmos de recomendação para garantir a proteção dos direitos à privacidade e a proteção de dados de usuários e sugerir como essas práticas podem ser implementadas.

[1]Graduanda em Direito pelo UNIPTAN. E-mail: marcela.guimaraes1998@gmail.com
[2]Professora do Curso de Direito no UNIPTAN. E-mail: erika.lasmar@uniptan.edu.br

Sendo assim, o intuito deste artigo é analisar a relação entre a garantia do direito de privacidade e a proteção de dados frente ao uso do algoritmo de recomendação de *e-commerce* sob a ótica da LGPD (BRASIL, 2018). Como resultado, pretende-se que esse trabalho contribua para aumentar a conscientização sobre a necessidade de proteção de dados e privacidade dos usuários e para fornecer recomendações para a implementação de medidas de segurança para garantir a integridade de dados dos usuários.

Consequentemente, o presente artigo estabeleceu como problema de pesquisa: quais as principais práticas recomendadas, de acordo com a LGPD (BRASIL, 2018), a *e-commerces* que utilizam algoritmos de recomendação para garantir a proteção dos direitos à privacidade e a proteção de dados de usuários e como implementá-las? E como objetivo geral: identificar as principais práticas recomendadas, de acordo com a LGPD (BRASIL, 2018), a *e-commerces* que utilizam algoritmos de recomendação para garantir a proteção dos direitos à privacidade e a proteção de dados de usuários. Para alcançar o objetivo geral, os objetivos específicos serão: O histórico da jornada que induziu à criação da LGPD (BRASIL, 2018), conceituar algoritmos de recomendações e como eles operam em *e-commerces*, identificar as principais práticas recomendadas para a proteção dos direitos à privacidade e proteção de dados e analisar a forma em que as práticas recomendadas podem vir a ser implementadas, por *e-commerces* que utilizam algoritmos de recomendação.

O presente estudo consiste em pesquisa aplicada de caráter exploratório, que visa a identificação das principais práticas recomendadas a garantir a proteção do direito à privacidade e a proteção de dados de usuários de *e-commerce* que utilizam algoritmos de recomendação. Nesse sentido, os resultados serão apresentados de forma qualitativa, a partir da coleta de informações de fontes secundárias, abordando artigos, sites e livros que explanam sobre o tema.

Este artigo encontra-se organizado em 5 tópicos. É apresentado um histórico da jornada que levou a criação da LGPD (BRASIL, 2018). Em seguida é definido o que é algoritmo, o conceito e as formas em que se dividem os algoritmos de recomendação. Posteriormente são expostas as principais práticas recomendadas pela LGPD (BRASIL, 2018). E após, apresenta as diretrizes para a implementação dessas práticas. E, por fim, são apresentadas as considerações finais.

2 O HISTÓRICO DA JORNADA QUE INDUZIU À CRIAÇÃO DA LGPD

O histórico da Lei Geral de Proteção de Dados (BRASIL, 2018) remonta a diversos acontecimentos mundiais que levaram à necessidade de uma regulamentação mais rígida sobre a proteção de dados. Um desses marcos foi o escândalo da Cambridge Analytica (OLIVEIRA, 2021), empresa britânica, que ofereceu serviços de assessoria para campanhas políticas como as eleições dos *EUA* em 2016 e o *Brexit*. Utilizando informações coletadas através de testes de personalidade e análises de usuários do Facebook, *Steve Bannon*, ex-chefe da companhia, em meados de 2014, formou estratégias políticas. O escândalo veio à tona em 2018, após o jornal *The Observer* receber denúncias e comprovar que a empresa gastou cerca de US $1 milhão (CADWALLADR; GRAHAM-HARRISONR, 2018) na coleta de dados pessoais dos usuários, incluindo informações sobre gostos, hábitos, profissão e localização. Os dados foram coletados pelo professor *Aleksandr Kogan* em um teste de personalidade, que também acabou coletando dados de amigos sem consentimento. *Christopher Wylie*, ex-funcionário da *Cambridge Analytica*, foi o responsável pelas denúncias e colaborou com as investigações (OLIVEIRA,2021).

Com o ocorrido, alguns países passaram a cogitar quanto à possibilidade de evitar futuros casos semelhantes e em como combater ameaças à democracia, o que fortaleceu o discurso para novas leis de proteção de dados dos usuários. Como a *General Data Protection Regulation* (GDPR), que substituiu a Diretiva de Proteção de Dados de 1995, que buscava proteger os indivíduos em relação ao processamento de seus dados pessoais e à livre circulação desses dados (XIMBRE, 2022). As preocupações crescentes em relação à proteção de dados, principalmente na ascensão dos direitos online de privacidade (XIMBRE, 2022) para estimular a economia digital na Europa, surgiram entre 2011 e 2012. Em 2014, o Parlamento Europeu deliberou acerca de adotar o projeto da *GDPR* 6), de forma unânime. Em 2015, no ano seguinte, o Conselho Europeu estabeleceu uma abordagem geral para a *GDPR* (*PE, 2016*), seguida de recomendações da AEPD (Autoridade Europeia para a Proteção de Dados). Isso gerou o plano de ação para a implementação da *GDPR* (*PE, 2016*) que foi publicado em 27 de abril de 2016, um prazo de dois anos para adequação, e entrou em vigor em 2018, ano em que ocorreu a divulgação do escândalo da *Cambridge Analytica*. A *GDPR* (*PE, 2016*) foi um marco importante nos últimos anos na União Europeia, pois fortaleceu a proteção de dados pessoais e promoveu a privacidade online, além de ocasionar um "efeito dominó" forçando, outros países e empresas que desejavam manter relações comerciais com a União Europeia, a exigência de conformidade com o regulamento. Isso significa que qualquer Estado que não possuísse uma legislação de proteção de dados equivalente poderia enfrentar obstáculos ou dificuldades para realizar negócios com eles. Esse cenário é especialmente desejável para a maioria das nações,

principalmente na América Latina, devido ao atual contexto econômico (PINHEIRO, 2023, p.6).

Neste mesmo período de 2011, no Brasil, foi aprovada a Lei 12.527/11 (BRASIL, 2011) que é a Lei de Acesso à Informação (SOARES, 2020), ela foi um passo importante para a criação da LGPD (BRASIL, 2018), pois estabeleceu regras para garantir a transparência do acesso às informações públicas. A partir daí, iniciaram-se discussões sobre a necessidade de uma legislação específica para a proteção de dados pessoais.

No ano de 2013, ocorreu um evento que teve um grande impacto na proteção e tratamento de dados pessoais, além de reforçar a necessidade de uma maior segurança em relação a esses dados. Foi revelado por *Edward Snowden*, em 2013, o uso do *software PRISM*, e outros similares, que monitoravam e vigiavam informações transmitidas na internet de forma global. Esses programas coletavam informações em larga escala, espionando não apenas terroristas, mas qualquer pessoa que transmitisse informações online, incluindo países e grandes empresas estrangeiras (SOARES, 2020). Um exemplo disso foi o que aconteceu com Dilma Rousseff, presidente do Brasil na época, que foi uma das muitas vítimas, mostrando o quão vulnerável a privacidade é na internet (SOARES, 2020). Partindo da discussão sobre a necessidade de uma legislação e o impacto deste vazamento foi colocado em tramitação, aqui no Brasil, o projeto de Lei n° 2126/11, que foi transformado na Lei 12.965/2014 (BRASIL, 2014) que é conhecida como o Marco Civil da Internet, “que apesar de não trazer consigo qualquer tipo de proteção prática quanto à espionagem internacional, tinha alguns conceitos e princípios a respeito da privacidade e da proteção de dados pessoais” (SOARES, 2020, p.13).

A Lei Geral de Proteção de Dados (BRASIL, 2018), n° 13.709/18, foi sancionada em 14 de agosto de 2018 para modernizar a então em vigor, Lei do Marco Civil da Internet (BRASIL, 2014). Inspirada pela *GPDR* (CARVALHO, 2019), também tem como objetivo proteger a privacidade dos cidadãos em relação ao uso de seus dados pessoais. A LGPD (BRASIL, 2018) entrou em vigor, no Brasil, em setembro de 2020, após um período de transição, regulamentando a forma como as empresas e organizações lidam com os dados pessoais de seus clientes e usuários. O objetivo da LGPD (BRASIL, 2018) é legislar, regulamentar e fiscalizar as empresas que precisam seguir regras sobre como coletar, armazenar e usar informações. Essas regras são feitas para nos proteger e garantir que a privacidade dos dados seja mantida (GOMES, 2019), além de assegurar o controle dos titulares dos dados sobre as informações coletadas e retidas, “podendo modificar, corrigir ou excluir as informações" (SOARES, 2020, p. 06). Sendo assim, a LGPD (BRASIL, 2018) veio para proteger os direitos fundamentais, como Patrícia Pinheiro define em seu livro:

> O espírito da LGPD é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança da segurança das informações, de outro lado, dentro do ciclo de vida do uso da informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis. (PINHEIRO, 2023, p. 3)

A Lei (BRASIL, 2018) conta com 10 capítulos e 65 artigos: Disposições Preliminares (Art. 1° ao 6°), Do Tratamento de Dados Pessoais (Art. 7° ao 16), Dos Direitos do Titular (Art. 17 ao 22), Do Tratamento de Dados Pessoais pelo Poder Público (Art. 23 ao 32), Da Transferência Internacional de Dados (Art. 33 ao 36), Dos Agentes de tratamento de Dados Pessoais (Art. 37 ao 45), Da Segurança e Boas Práticas (Art. 46 a 51), Da Fiscalização (Art. 52 ao 54), Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (Art. 55 ao 59) e Disposições Finais e Transitórias (Art. 60 ao 65).

Para o presente trabalho fica em evidência o art. 2°, artigo que aborda os fundamentos da proteção de dados:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018)

Fundamentos estes que têm ligação com o conteúdo da Constituição Federal de 1988 (BRASIL, 1988) sendo então indispensáveis.

O art. 5° (BRASIL, 2018) que aborda a conceituação dos termos utilizados na Lei, para um melhor entendimento deles, em 19 incisos. Muito importante não só para a Lei como para o presente artigo os seguintes incisos:

> Art. 5º Para os fins desta Lei, considera-se:
> [...] XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
> [...] XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais

> que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; [...] (BRASIL, 2018)

E o Art. 6°, importante assim como os fundamentos e a conceituação dos termos, que aborda os princípios que regem a Lei Geral de Proteção de Dados (BRASIL, 2018). Podemos dividir os princípios em três partes, sendo os três primeiros sobre a preparação para o uso dos dados pessoais, os quatro seguintes sobre a transparência no uso de dados e os três últimos sobre a segurança e responsabilidade. Totalizando dez princípios, que além da boa-fé são:

> Art. 6° [...]
> I - finalidade[...]
> II - adequação[...]
> III - necessidade[...]
> IV - livre acesso[...]
> V - qualidade dos dados[...]
> VI - transparência[...]
> VII - segurança[...]
> VIII - prevenção[...]
> IX - não discriminação[...]
> X - responsabilização e prestação de contas[...]; (BRASIL, 2018)

Desta forma, é importante destacar que a LGPD (BRASIL, 2018) é uma legislação em constante evolução e que sua aplicação requer o envolvimento de profissionais protegidos e comprometidos com a proteção dos dados pessoais. O cumprimento da lei não é uma tarefa fácil, mas é fundamental para a proteção da privacidade e segurança dos dados pessoais dos cidadãos.

3 CONCEITUAR ALGORITMOS DE RECOMENDAÇÕES E COMO ELES OPERAM EM *E-COMMERCES*

Antes de tudo, é importante definirmos o que é e como funcionam os algoritmos computacionais. A ideia de algoritmo, apesar de hoje em dia ser utilizado amplamente nos computadores modernos, vem de muito tempo antes. A palavra tem origem no Século XII, pelo matemático Muhammad ibn Musa al-Khwarizmi com seu livro traduzido para o latim: "Algoritmi de número Indorum" ("Al-Khwarizmi sobre os números dos indianos") (GOMES, 2010).

Um “algoritmo é uma sequência finita de instruções, bem definidas e não-ambíguas” (Gomes, 2010, p. 2), que descrevem passo a passo de um processo computacional para resolver um determinado problema ou realizar uma determinada tarefa. Pode ser descrito também, por

um conjunto de regras que podem ser seguidas para realizar uma determinada ação e resolver um problema específico (GILLESPIE, 2018), gerando o mesmo resultado por qualquer um que siga esses passos.

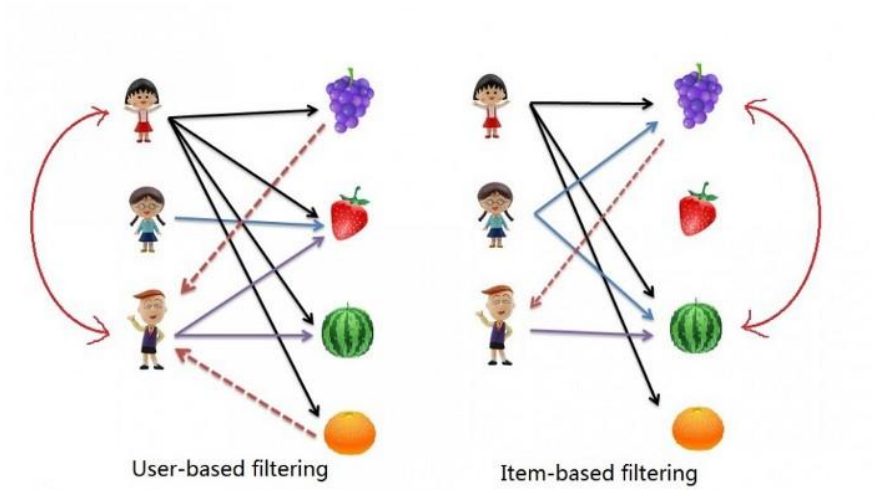
Desde a criação do conceito de algoritmos e suas aplicações nos computadores, muitas técnicas foram desenvolvidas ao longo dos anos. Uma das importantes ferramentas conceituais foi sobre a Inteligência artificial. A ideia de criar comportamentos computacionais semelhantes à de humanos teve início logo após a Segunda Guerra por *Alan Turing* com o artigo "*COMPUTING MACHINERY AND INTELLIGENCE*". (GOMES, 2010). Ainda na década de 50, também foi criado a ideia do aprendizado de máquina por *Arthur Lee Samuel*, que, além de conceituar que máquinas poderiam aprender por conta própria a partir de dados, criou um jogo de damas que realmente tomava decisões baseados nos aprendizados ao longo das rodadas. (CARVALHO, 2017).

Os algoritmos de recomendação utilizam-se de técnicas de aprendizado de máquina para recomendar produtos aos clientes baseado em possíveis interesses dos usuários (TAKAHASHI; HIRATA, 2015). Para inferir quais produtos devem ser recomendados para o usuário, os sistemas de recomendação utilizam os dados de comportamento tanto da pessoa, quanto de outras pessoas que também utilizam o sistema. A recomendação pode ser utilizada tanto para melhorar a experiência do cliente, oferecendo produtos e ofertas relevantes para ele, quanto também para obter vantagem competitiva (BORGES, 2016) aumentando a probabilidade de um cliente adquirir certo produto.

Existem 3 grupos de algoritmos para se criar sistemas de recomendação, que são: filtragem colaborativa, filtragem baseada em conteúdo e filtragem híbrida.

A filtragem colaborativa é utilizada em *e-commerces*, no formato de quem comprou X, também pode se interessar/comprar Y, ou recomendações similares. O sistema identifica padrões e semelhanças entre usuários que já interagiram ou compraram determinado produto anteriormente e também oferece outros produtos que esse grupo de usuários possam se interessar (TAKAHASHI; HIRATA, 2015). Desta forma, “a recomendação dos itens ao usuário é feita levando-se em consideração as preferências desse usuário e as preferências dos usuários que são semelhantes a ele” (BARBOSA, 2014, p. 10) , como podemos observar na figura 1:

Figura 1 - Filtragem colaborativa

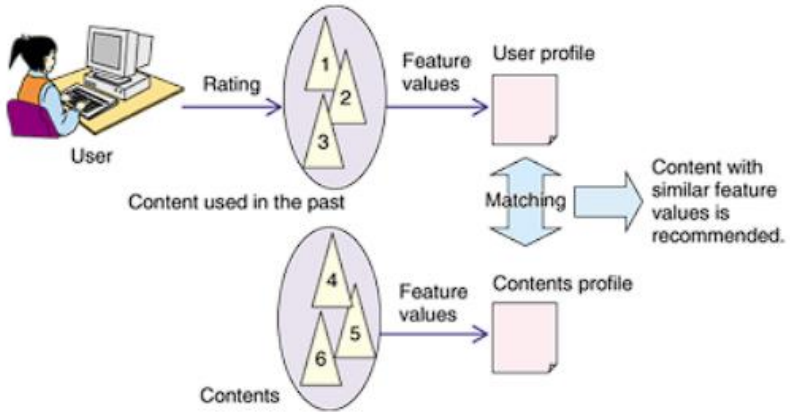


Fonte: Ilumeo

A filtragem colaborativa possui dois tipos, como visto na imagem, no primeiro momento temos a filtragem colaborativa onde o sistema encontra usuários parecidos com base na similaridade das interações dos outros usuários com os itens, e recomenda as frutas que os primeiros usuários parecidos escolheram no passado. Já no segundo momento, ao contrário da anterior, ela não busca encontrar usuários similares e sim encontrar as frutas parecidas a partir da escolha dos usuários. Em ambos os casos, é utilizado o comportamento de outros clientes, além do seu próprio comportamento.

Já a filtragem baseada em conteúdo utiliza-se de itens similares aos que foram interagidos pelo próprio usuário no passado, não levando em consideração outros clientes. Esse processo consiste em cruzar os interesses e preferências do perfil do usuário com os atributos dos produtos para recomendá-los ao cliente (COSTA et al; 2013). Desta forma é feita uma "análise da correlação entre o conteúdo dos itens com o perfil do usuário para recomendar itens relevantes e descartar os itens não pertinentes" (BEZERRA, 2002). Um exemplo que pode ser dado é, que caso você procure por algum acessório automobilístico, pode aparecer frequentemente para você outros acessórios que você também possa se interessar e até mesmo, o mesmo produto (TAKAHASHI; HIRATA, 2015). Como observado na figura 2:

Figura 2 - Filtragem baseada em conteúdo

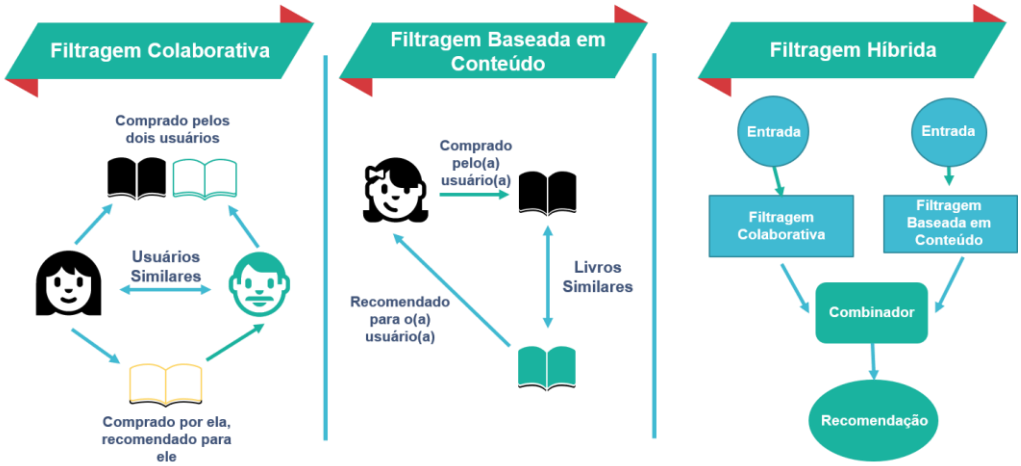


Fonte: TAKAHASHI; HIRATA, 2015.

O conteúdo de acesso e de compras de um usuário, feito no passado é confrontado com as características dos demais produtos da base de dados, caso coincida com conteúdo similares, estes serão recomendados ao usuário por serem semelhantes ou o mesmo item já interagido.

E por fim a filtragem híbrida, que combina ambas técnicas definidas anteriormente buscando "tirar proveito das vantagens de cada uma delas de modo a desenvolver um sistema que recomende o conteúdo mais adequado para o usuário" (ROLIM et al., 2017, p. 727). Um combinador dos resultados pode ser aplicado após serem feitas as duas técnicas ou pode ser aplicado uma abordagem após a outra, gerando resultados mais precisos (TAKAHASHI; HIRATA, 2015). Como apresentado na figura abaixo:

Figura 3 - Filtragem híbrida



Fonte: VINISKI, 2021.

Podemos então inferir recomendações tanto no comportamento de outros usuários parecidos com o seu, recomendando itens que eles se interessaram, quanto na similaridade de produtos, para lhe oferecer produtos relevantes com a sua busca recente. Para isso, deve-se

coletar os dados dos usuários e aplicar uma ou mais técnicas de recomendação. Mas junto a coleta destes dados e aplicação das técnicas de recomendação de algoritmos surgem as preocupações quanto à privacidade e proteção de dados pois:

> [...] questões relacionadas à privacidade e proteção de dados são um dos maiores desafios das tecnologias de recomendação, já que esses sistemas necessitam de uma enorme quantidade de informações pessoais e de comportamento dos usuários para alcançar uma percepção profunda de suas preferências e, assim, prever itens de interesse. (SILVA, 2021, pág.25)

Por isso, os *e-commerces* devem sempre ficar atentos para preservar os direitos dos seus usuários, utilizando-se de boas práticas de desenvolvimento e arquitetura de sistemas, além, claro, da segurança da informação.

4 PRINCIPAIS PRÁTICAS PARA GARANTIR A PROTEÇÃO DOS DIREITOS À PRIVACIDADE E A PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (BRASIL, 2018) estabelece uma série de práticas recomendadas para garantir a proteção dos direitos à privacidade e proteção de dados dos usuários. Algumas das principais práticas são:

O Consentimento, onde as empresas devem obter o consentimento explícito dos usuários antes de coletar, armazenar, processar ou compartilhar seus dados pessoais. Para que o consentimento seja considerado válido, ele deve ser expresso de forma clara, inequívoca e específica, sem ambiguidades, isso significa que as empresas devem informar aos titulares dos dados, de forma clara e transparente, as finalidades para as quais os dados serão utilizados, quem terá acesso aos dados e por quanto tempo eles serão armazenados. O consentimento também deve ser livre, ou seja, os titulares dos dados devem ter a opção de recusar o consentimento sem sofrer qualquer tipo de prejuízo ou discriminação. Além disso, o consentimento deve ser revogável a qualquer momento, e as empresas devem oferecer meios simples e eficazes para que os titulares dos dados possam revogar o consentimento (TEFFÉ; TEPEDINO, 2020). Sendo assim, o consentimento é um elemento fundamental para garantir a proteção dos direitos à privacidade e proteção de dados dos usuários, e deve ser obtido de forma clara, livre e específica, de acordo com os requisitos estabelecidos pela LGPD.

A transparência, que faz com que as empresas sejam transparentes sobre como coletam, armazenam, processam e compartilham os dados pessoais dos usuários. Isso inclui divulgar as

finalidades para as quais os dados serão utilizados, o tempo de retenção dos dados e os direitos dos usuários em relação aos seus dados. Fornecendo, então, aos titulares dos dados uma política de privacidade clara, simples e acessível, que explique de forma detalhada como os dados pessoais serão tratados (GALHARDO, 2022) e informando a esses titulares sempre que houver mudanças significativas na política de privacidade ou no tratamento de dados pessoais. Consequentemente, a transparência ajuda a aumentar a confiança dos usuários nas empresas (NICASTRO, 2021), demonstrando que elas estão comprometidas em proteger a privacidade e os dados pessoais dos titulares.

A segurança, onde empresas devem adotar medidas técnicas e organizacionais para garantir a segurança dos dados pessoais dos usuários, evitando o acesso não autorizado, a perda, a destruição ou a divulgação indevida dos dados. Aderindo medidas de segurança apropriadas para proteger os dados pessoais que coletam e tratam. Caso haja algum incidente envolvendo violação da segurança a empresa deve notificar os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2018) sobre o ocorrido (BENEDITO, 2021), bem como tomar medidas para minimizar os impactos desse incidente.

E a minimização de dados que aborda que as empresas devem coletar apenas os dados pessoais necessários para atingir as finalidades específicas para as quais os dados são coletados. Além disso, devem excluir os dados pessoais quando não forem mais necessários para a finalidade específica para a qual foram coletados (BUCHAIN, 2022).

Essas são as principais práticas recomendadas pela LGPD para garantir a proteção dos direitos à privacidade e proteção de dados dos usuários. É importante que os *e-commerces*, que é o caso do presente artigo, se atentem e implementem elas para que estejam em conformidade com a legislação.

5 DIRETRIZES PARA A APLICAÇÃO DAS PRINCIPAIS PRÁTICAS RECOMENDADAS DA LGPD EM *E-COMMERCES*

A Lei Geral de Proteção de Dados (BRASIL, 2018) estabelece uma série de práticas recomendadas que devem ser adotadas por empresas, incluindo *e-commerces*, para garantir a proteção dos direitos à privacidade e proteção de dados dos usuários. Dentre essas práticas, destacam-se o consentimento, a transparência, a segurança e a minimização de dados, já mencionados acima. A implementação destas práticas em *e-commerces* pode ajudar a proteger a privacidade e os dados pessoais dos usuários, garantindo que as empresas coletem apenas os dados necessários e adequados para a finalidade específica do tratamento e ofereçam

transparência e segurança aos titulares dos dados pessoais, ou seja, a implementação dessas práticas recomendadas pode ajudar a garantir a proteção da privacidade e dos dados pessoais dos usuários em *e-commerce*, garantindo a conformidade com a LGPD (BRASIL, 2018) e a manutenção da confiança do público em relação à ele. Para implementar essas práticas, o *e-commerce* pode adotar abordagens como:

O *Privacy by Design* (Privacidade desde o projeto) em que "a escolha da tecnologia utilizada na oferta de produtos e serviços é pensada, desde o início, para a proteção dos dados pessoais." (FRAZÃO, et al., 2019, p. 710), isto é, incorporar a privacidade e a proteção de dados desde a concepção de um produto ou serviço. O *Privacy by Design* (PbD) é um conceito de proteção à privacidade que foi desenvolvido por *Ann Cavoukian*, que era comissária de informações e privacidade de *Ontário*, Canadá, em 1990. O *Privacy by Design* é um modelo proativo de proteção à privacidade que se concentra em garantir que a privacidade seja considerada em todas as fases do ciclo de vida dos dados, desde a coleta até a disposição. Isso significa que a privacidade é considerada em cada aspecto de um sistema, incluindo sua arquitetura, configuração, políticas e procedimentos (MARRAFON; COUTINHO, 2020). São sete os princípios fundamentais do *Privacy by Design* (CAVOUKIAN, 2009), sendo eles: a) A proatividade que é a abordagem baseada em medidas preventivas, em vez de reativas, buscando prever e evitar a ocorrência de eventos que possam violar a privacidade dos usuários, em vez de lidar com as consequências após o fato; b) A privacidade como padrão garantindo que a privacidade seja protegida de forma automática e padrão independentemente da ação ou inação do indivíduo; c)A privacidade incorporada ao design resultando na privacidade como um componente essencial da funcionalidade principal do sistema, e não um recurso adicional, tornando-se, então, parte integrante do sistema, sem comprometer ou diminuir a funcionalidade; d) Uma funcionalidade completa visando uma abordagem que satisfaça a todos de maneira positiva, sem a necessidade de sacrificar um interesse em detrimento do outro; e) A segurança de ponta a ponta garantindo um gerenciamento seguro do ciclo de vida das informações, desde a coleta até a destruição, oferecendo segurança total para as informações envolvidas; f) A visibilidade e transparência que além de promover a verificação, garantindo a transparência e a prestação de contas para todas as partes interessadas envolvidas, incentiva a confiança; g) O respeito pela privacidade do usuário mantendo o foco e priorizando a proteção de seus interesses, fornecendo medidas para garantir a privacidade e a escolha segura (CAVOUKIAN, 2009).

Conforme Marrafon e Coutinho abordam em seu artigo, dentre os benefícios da prática valem ressaltar:

> [...] (a) vantagem competitiva no mercado contra outros projetos que não ofereçam respeito à privacidade dos dados pessoais do consumidor ou cliente; (b) maior confiança e lealdade do consumidor; (c) garantias de eficiência do processo e mitigação dos riscos como resultado do processamento de dados pessoais estritamente necessários aos fins comerciais previamente expostos; (d) minimização de riscos e, por conseguinte, dos custos derivados de violações à privacidade e segurança de dados; (e) a assunção de postura proativa na implementação e no desenvolvimento de produtos ou serviços em conformidade com os valores fundamentais da privacidade, autonomia, igualdade e devido processo legal; e, por fim, (f) os consumidores tratarão a privacidade de seus dados pessoais como questão de negócio, e não um problema de compliance. (MARRAFON; COUTINHO, 2020, p.976-977)

Além de ajudar as empresas, ou melhor, os *e-commerces*, seguindo a lógica do presente artigo, a se adaptarem às regulamentações como a *General Data Protection Regulation* da União Europeia e a Lei Geral de Proteção de Dados no Brasil. Em síntese, o *Privacy by Design* é uma abordagem proativa para a proteção da privacidade e dos dados pessoais, que promove a incorporação da privacidade desde o início do design de sistemas, processos e produtos. Isso pode ajudar as empresas a evitar riscos e vulnerabilidades à privacidade e se adaptarem às regulamentações de privacidade.

O *Data Minimization* (Minimização de dados) que tem como objetivo minimizar a quantidade de dados pessoais coletados, processados e armazenados por um *e-commerce*, exigindo que esses dados sejam processados apenas para finalidades especificadas, explícitas e legítimas e que não sejam processados posteriormente de maneira incompatível com essas finalidades (BIEGA, 2020, p. 400). É importante evidenciar que a minimização de dados é uma responsabilidade dos controladores de dados, ou seja, das entidades que decidem como e por que os dados pessoais são recolhidos, processados e armazenados e que

> [...] quaisquer políticas desposadas por controladores que busquem reter todo e qualquer tipo de informação do titular, sejam elas ou não pertinentes com a finalidade econômica do negócio jurídico havido entre eles, possivelmente será considerada ilícita. (BUCHAIN, 2022, p. 54)

Sendo assim, ao coletar apenas os dados necessários, é possível reduzir os riscos de violação de privacidade e o risco de vazamento de informações pessoais dos usuários.

O treinamento e a conscientização dos colaboradores sobre a importância da privacidade e proteção de dados, para garantir que todos os colaboradores estejam alinhados com as práticas recomendadas e possam contribuir para a proteção dos dados pessoais dos usuários.

> Ao conscientizar seus colaboradores, instituições que realizam treinamentos sobre a LGPD obtêm efeitos positivos e diminuição das vulnerabilidades, mas essa conscientização precisa ser realizada desde a diretoria, até a portaria do prédio da empresa, com linguagem de acordo com a função do colaborador, para ele poder saber lidar com situações em que tratem de dados pessoais sem colocar a empresa e/ou seus dados pessoais em risco. (LEITE, 2021, p.35-36)

Nesse sentido, ao capacitar os colaboradores para entenderem a importância da privacidade e da proteção de dados, bem como as obrigações legais e as melhores práticas para garantir esses direitos, as empresas podem promover uma cultura de privacidade e responsabilidade no tratamento de dados pessoais. Além disso, ao realizar treinamentos regulares e conscientizar os colaboradores sobre as práticas de privacidade e proteção de dados, as empresas podem demonstrar o seu compromisso com o princípio de *Accountability* (Responsabilização/ Prestação de contas) (NÓBREGA, 2021) e prestar contas sobre as suas práticas de tratamento de dados pessoais. Dessa forma, os colaboradores se tornam aliados na proteção da privacidade e da proteção de dados pessoais e contribuem para a construção de uma cultura de confiança entre a empresa e os seus clientes, usuários.

Além das implementações citadas acima, vale evidenciar, de forma sucinta, que o *e-commerce* pode realizar um mapeamento dos dados pessoais coletados para entender a natureza e a finalidade do tratamento desses dados e identificar possíveis riscos à privacidade e à proteção dos dados pessoais. Também pode realizar uma análise de legítimo interesse para avaliar se o tratamento de determinados dados pessoais é justificado em função de um interesse legítimo do controlador ou de terceiros, como a melhoria da experiência do usuário ou a prevenção de fraudes.

Cabe destacar ainda a importância do Relatório de Impacto à Proteção de Dados (BRASIL, 2018), visto anteriormente no art. 5°, inciso XVII, da LGPD (BRASIL, 2018), como sendo uma ferramenta utilizada para avaliar e documentar os riscos relacionados ao tratamento de dados pessoais em determinadas atividades ou projetos, e estabelecer medidas para mitigar esses riscos.

Tem ainda a anonimização, que é o processo de tornar os dados pessoais irreversivelmente irreconhecíveis e não associáveis a um indivíduo específico. A LGPD (BRASIL, 2018) exige que os dados pessoais sejam anonimizados sempre que possível, para proteger a privacidade e evitar a identificação de indivíduos sem consentimento.

Dessa forma, é essencial que os *e-commerces* fiquem atentos ao utilizar algoritmos de recomendação e que ao utilizarem adotem as práticas recomendadas de proteção de dados pessoais e cumpram as obrigações previstas na LGPD (BRASIL, 2018), para evitar possíveis sanções e garantir a proteção dos dados pessoais dos titulares.

6 CONSIDERAÇÕES FINAIS

Conforme apresentado ao longo do artigo, é evidente a importância da utilização de práticas recomendadas pela LGPD (BRASIL, 2018) para garantir a proteção ao direito à privacidade e à proteção de dados dos usuários, já que a não utilização dessas práticas podem impactar fortemente as empresas. Nesta concepção, os *e-commerces* que utilizam os algoritmos de recomendações devem aderir junto a eles essas práticas, visto que, com isso, além de recomendar produtos baseado em possíveis interesses dos usuários, eles vão garantir a proteção e segurança dos mesmos.

A coleta e o tratamento de dados contêm riscos inerentes tanto às tecnologias utilizadas quanto ao fator humano, mas com a LGPD (BRASIL, 2018) e as boas práticas recomendadas por ela, para a proteção de dados e privacidade, esses riscos vêm sendo mitigados. Com isso, as técnicas apresentadas no quarto tópico que incluem transparência no uso de algoritmos, consentimento explícito, medidas de segurança, acesso/controle dos dados pelos usuários e retenção limitada de dados, mais as formas de implementação das mesmas, visto no quinto tópico, podem ajudar a construir a confiança dos usuários e evitar riscos ou uso inadequado de dados pessoais, visando garantir os princípios regidos pela Lei.

Em contrapartida, ressalta-se que apesar dos inúmeros benefícios trazidos pela aderência à regulamentação da LGPD, algumas empresas podem vir a não se adequarem. Fato este, que decorre em prejuízos, sejam jurídicos, uma vez que vai contra a previsão legal e incorrerá em sanções, criminais e administrativas, sejam financeiros, ao passo que os consumidores que se encontrando diante das duas opções, dará preferência, na maioria das vezes, àquela que lhe assegura a proteção de seus dados.

Outrossim, não bastantes os danos acima indicados, cumpre pontuar outro ao qual os estabelecimentos que seguem os trâmites impostos pela Lei, estão expostos: malefícios advindos de eventual vazamento dos dados. Indubitavelmente, as empresas que se amparam na norma, devem empenhar esforços na profissionalização capacitada daqueles responsáveis pelo setor de proteção, já que para lidar com a matéria, deve-se apresentar reconhecida capacidade para exercê-la. Desta forma, ocorrendo o vazamento dos dados fornecidos, em tese protegidos, há logicamente que se falar em consequências danosas à entidade.

Logo, buscando reforçar a preservação das informações pessoais fornecidas, demanda-se futuras pesquisas para evitar riscos inerentes à natureza. Carece de análises acerca do período de conservação do material, maneira que serão inutilizados/excluídos, decurso do prazo de

responsabilização das empresas, entre outras questões hábeis a auxiliar na ampliação do resguardo de dados pessoais dos consumidores que os forneceram.

REFERÊNCIAS

BRASIL. **Lei N° 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Diário Oficial da União, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 22 de mar. de 2023.

Brasil. Lei N° 12.527, de 18 de novembro de 2011. **Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências**. Brasília, DF: Diário Oficial da União, 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso em: 22 de mar. de 2023.

Brasil. Lei N° 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília, DF: Diário Oficial da União, 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 22 de mar. de 2023.

BARBOSA, Carlos Eduardo Martins. **Estudo de técnicas de filtragem híbrida em sistemas de recomendação de produtos**. 2014. 99f. Monografia (Ciência da Computação) - Centro de Informática, Ciência da Computação, Universidade Federal de Pernambuco, 2014.

BENEDITO, Matheus Braga. **Lei geral de proteção de dados: uma análise sobre os direitos dos titulares e os deveres das organizações perante a lei**. 2021. 15f. TCC (Ciências da Computação) - Centro de Engenharia Elétrica e Informática da Universidade Federal de Campina Grande. 2021.

BEZERRA, Byron Leite Dantas. **Estudo de algoritmos de filtragem de informação baseados em conteúdo**. 2002. 45f . Trabalho de Conclusão de Curso (Graduação em Inteligência Artificial) - Universidade Federal de Pernambuco. 2002.

BIEGA, Asia J. et al. Operationalizing the legal principle of data minimization for personalization. In: **Proceedings of the 43rd international ACM SIGIR conference on research and development in information retrieval**. 2020. p. 399-408. July. 2020.

BORGES, Fabio Roberto Ferreira Borges. **O efeito de recomendações e argumentos de prova social na intenção de compra e experiência do cliente no comércio eletrônico**. 2016. 354f . Tese (Doutorado em Administração) - Faculdade de Ciências Econômicas da Universidade Federal de Minas Gerais. Belo Horizonte. 2016.

BUCHAIN, Luiz Carlos. Minimização e proporcionalidade na coleta de dados. **Direitos Democráticos & Estado Moderno**, [S. l.], v. 2, n. 5, p. 51-68, mai./ago. 2022.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian**, Reino Unido, 17 mar. 2018. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em 22 de mar. de 2023.

CARVALHO, G. P.; PEDRINI, T. F. Direito à Privacidade na Lei Geral de Proteção de Dados Pessoais. **Revista da ESMESC**, [S. l.], v. 26, n. 32, p. 363–382, 2019.

CARVALHO, Samuel Domingues Santos Costa. **Heurística auxiliada por Aprendizagem Automática aplicada a problemas de Escalonamento**. 2017. 71f. Dissertação (Mestrado em Engenharia Informática) - Instituto Politecnico do Porto, Portugal, 2017.

CAVOUKIAN, Ann. Privacy by design: The 7 Foundational Principles. **Privacy by design.** Canadá. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. 2009. Acesso em 03 de maio de 2023.

COSTA, Evandro; AGUIAR, Janderson; MAGALHÃES, Jonathas. Sistemas de Recomendação de Recursos Educacionais: conceitos, técnicas e aplicações. **Jornada de Atualização em Informática na Educação**, v. 1, n. 1, p. 57-78, 2013.

FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. [S. l.]. Thomson Reuters Brasil, 2019.

GALHARDO, Jessica Aparecida Ferreira. **Lei geral de proteção de dados pessoais: desafios e perspectivas de sua implementação no Brasil**. 2022. 64f. TCC (Direito) Departamento de Ciências Jurídicas da Universidade de Taubaté, 2022.

GILLESPIE, Tarleton. A relevância dos algoritmos. **§ Parágrafo**. São Paulo. v. 6, n. 1, p. 95-121, jan./abr. 2018.

GOMES, Heloisa dos Santos. **Lei Geral De Proteção de Dados (LGPD): uma análise dos impactos da lei na cultura e tratamento de dados no Brasil**. 2019. 28f. TCC (Tecnólogo em Análise e Desenvolvimento de Sistemas) - Universidade do Sul de Santa Catarina, 2019.

GOMES, D. dos S. Inteligência Artificial: conceitos e aplicações. **Olhar Científico**. v1, n. 2, p. 234-246, 2010.

ILUMEO. **Data science company.** Disponível em: https://ilumeo.com.br/. acesso em 02 de maio de 2023.

LEITE, Vanessa Rodrigues. **Lei Geral de Proteção de Dados (LGPD): características e aplicações na Biblioteconomia e Ciência da Informação**. 2021. 52f. Monografia (Biblioteconomia) - Universidade Federal do Rio Grande do Norte, Centro de Ciências Sociais Aplicadas, Departamento de Ciência da Informação. Natal, RN, 2021.

MARRAFON, Marco Aurélio; COUTINHO, Luiza Leite Cabral Loureiro. Princípio da privacidade por design: fundamentos e efetividade regulatória na garantia do direito à proteção de dados. **Revista Eletrônica Direito e Política**, v. 15, n. 3, p. 955-984, 2020.

NICASTRO, Marcella Lomba; DOS SANTOS, Aguinaldo. Modelo teórico para diagnóstico da transparência em serviços: uma proposta para o setor de alimentos. **Estudos Em Design**, v. 29, n. 1, p. 65-81, 2021.

NÓBREGA, Fernando S.; FERREIRA, Loren O. **Guia de Boas Práticas: Aplicação de Accountability na gestão de dados em Cidades Inteligentes**. 2021. 13f. Tese (Computação e Informática) Faculdade de Computação e Informática Universidade Presbiteriana Mackenzie – São Paulo, 2021.

OLIVEIRA, Letícia Costa. **O uso de dados pessoais na era digital como forma de manipulação social e ameaça à democracia: um estudo de caso da Cambridge Analytica**. 2021. 63f. TCC (Graduação em Relações Internacionais) - Escola de Direito e Relações Internacionais da Pontifícia Universidade Católica de Goiás, 2021.

PARLAMENTO EUROPEU (PE). **General Data Protection Regulation.** Regulamento 2016/679. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN> . Acesso em: 23 mar. de 2023.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n.13.709/2018 (LGPD)**. 4. ed. - São Paulo: SaraivaJur, 2023.

ROLIM, Vitor et al. Um estudo sobre sistemas de recomendação de recursos educacionais. In: **Anais dos Workshops do Congresso Brasileiro de Informática na Educação**. 2017. p. 724-733.

SILVA, Paula Guedes Fernandes da. **Novas Tecnologias, Big Tech e Potenciais violações De Direitos Humanos: o Caso Dos Sistemas De recomendação**. 2021. 60f. Tese (Doutorado em Direito) - Universidade Catolica Portugesa, Portugal, 2021.

SOARES, Rafael Ramos. **Lei geral de proteção de dados–LGPD: direito à privacidade no mundo globalizado**. 2020. 31f. Monografia (Curso de Direito) - Pontifícia Universidade Católica de Goiás, 2020.

TAKAHASHI, Marcos M.; HIRATA JR, Roberto. **Estudo comparativo de Algoritmos de Recomendação**. Universidade de São Paulo. Instituto de Matemática e Estatística Bacharelado em Ciências da Computação, fev 2015.

TEFFÉ, Chiara Antonia Spadaccini de; TEPEDINO, Gustavo. O consentimento na circulação de dados pessoais. **Revista Brasileira de Direito Civil**, v. 25, n. 03, p. 83-83, 2020.

VINISKI, Antonio D. **O que fazem os sistemas de recomendação? Linkedin,** 07 jan. 2021. Disponível em: <https://www.linkedin.com/pulse/o-que-fazem-os-sistemas-de-recomenda%C3%A7%C3%A3o-antonio-david-viniski?trk=public_profile_article_view> . Acesso em: 25 de maio de 2023.

XIMBRE, Bernardo Ferreira Santos. **Explorando princípios da general data protection regulation, Lei Geral de Proteção de Dados e diretrizes éticas da inteligência artificial em repositórios open source**. 2022. 56f. Monografia (Curso de Engenharia da Computação) - Instituto de Ciências Exatas, Departamento de Ciência da Computação da Universidade de Brasília, 2022

.