1. Introdução:

A pandemia do COVID-19 impactou nas escolas e no ensino, e exige-se uma reinvenção da escola e dos professores. É momento de criar, inventar, romper com padrões e premissas e utilizar novas estratégias. O uso de plataformas levam a internet nesse momento para dentro da escola e das casas de professores e alunos. Não se trata apenas de converter o ensino presencial para as atividades virtuais, mas utilizar as ferramentas e plataformas como uma oportunidade pedagógica (BOTO, 2020).

O Ministério da Educação define a Educação à Distância como:

> Modalidade educacional na qual alunos e professores estão separados, física ou temporalmente e, por isso, faz-se necessária a utilização de meios e tecnologias de informação e comunicação. Essa modalidade é regulada por uma legislação específica e pode ser implantada na educação básica (educação de jovens e adultos, educação profissional técnica de nível médio) e na educação superior (BRASIL, 2005).

A Educação à distância parte de um conceito mais abrangente, e dentro dele está o conceito de Educação Online, o qual é definido por ações de ensino aprendizagem que fazem uso de meios digitais que possibilitam interações e atividades textuais entre os aprendizes e educador, entre aprendizes e/ou aprendizes e conteúdos (SANTOS, 2009; MORAN, 2003).

Assim, diante da indicação do distanciamento social as escolas passaram a adotar a Educação remota de Emergência, a qual acontece, quando as instruções e conteúdos que antes eram entregues no modo presencial, passam a ser entregues no modo online, uma adaptação da Educação Online, que tem a premissa de ser preparada, planejada e desenhada com tempo hábil antes de ser implementada (HODGES et al, 2020).

A partir dessa transição das atividades presenciais para a educação online, surge um problema que vai além das questões pedagógicas: a segurança e a privacidade dos dados dos alunos e professores nesse contexto. Têm-se sido utilizadas plataformas comerciais de educação como Zoom®, Hangouts®, ambientes educacionais do Google®,

ambientes virtuais como o Coursera, plataforma da Microsoft Teams®, entre outros. A preocupação ocorre quando os dados se tornam sujeitos a monitoramentos pouco transparentes e que são coletados, analisados e vendidos para empresas que podem direcionar as ações de Marketing a fim de oferecer produtos ou serviços baseados nos comportamentos dos clientes em potencial (JUNQUEIRA, 2020).

Logo, deve-se refletir sobre a luz da ética e moral para o uso e acesso de dados. Lembrando que essa palavra é derivada do grego *éthos*, que indica costumes, hábito, caráter, modo de ser de uma pessoa (RENAUD, 2001), e o significado de moral, derivado do latim *mos*, que remete a normas do cotidiano e leis (TUGENDHAT,1999), esses dois aspectos possuem uma relação intrínseca e recomenda-se um equilíbrio entre elas, já que ambas devem estar no campo da razão e do conhecimento dos indivíduos (PEDRO, 2014).

Na área da tecnologia existem poucas diretrizes éticas, diferentemente de áreas da ciência e saúde que têm legislações rigorosas em relação aos aspectos éticos envolvendo seres humanos (BRASIL, 2012). A Sociedade Brasileira de Computação descreve o Código de Ética do Profissional de Informática, o qual prevê: *"Art. 7: Respeitar a legislação vigente, o interesse social e os direitos de terceiros e Art. 10: Não praticar atos que possam comprometer a honra, a dignidade, privacidade de qualquer pessoa como dever do Profissional de Informática"* (SOCIEDADE BRASILEIRA DE COMPUTAÇÃO, 2013).

Temos uma tríade de atributos que devem ser respeitados durante a análise, planejamento e implementação da segurança em informações que desejamos proteger, são elas: confidencialidade, integridade, disponibilidade. Outros itens importantes são a autenticidade e com a evolução do comércio eletrônico e a privacidade é primordial quando se trabalha com dados na Educação à Distância (REIS, 2010).

A exposição aos cibercrimes tem sido comum diante do uso das tecnologias de informação, e deve-se lembrar que por trás dessas ações, estão indivíduos que ferem os princípios da ética e da moral, e utilizam-se de sistemas de segurança frágeis para acessarem e utilizarem informações. E nem sempre a norma moral está em consonância com a norma jurídica, pois a primeira está relacionada ao indivíduo e seus valores, a segunda relacionada à legislação e independe se o indivíduo concorda ou não, sofrerá as penalidades se não obediência (LIMA et al., 2016).

Seguindo nessa lógica da norma jurídica, o Brasil criou a Lei de Proteção nº 13.709/18, ou Lei de Proteção de Dados Pessoais e Privacidade (LGPD), que estabelece normas rigorosas para a proteção dos dados pessoais é recente e deve impactar nas relações com os dados tanto no ambiente privado como público (BRASIL, 2018). De forma geral a Legislação não abrange a educação à distância ou a educação online, mas alunos e pais devem estar atentos às políticas de privacidade das ferramentas ou aplicativos utilizados no ensino.

Diante de um cenário tão desafiador e de tantas mudanças, no momento atual, este estudo procurou identificar quais os aspectos da ética, privacidade e segurança na Educação online/distância utilizadas durante a pandemia no Brasil.

Ainda temos pouca literatura com a temática de regulamentações sobre Educação online e políticas de segurança de dado, haja visto as legislações existentes são da última década.

Um campo vasto e de muitas demandas devem surgir a partir da pandemia para a Educação Mundial e grandes oportunidades de pesquisas e estudos nessa temática, que tem sido pouco explorada.

2. Objetivo Geral:

Discutir o contexto da educação à distância, face a questão da Pandemia no Brasil e apontar os aspectos da ética, segurança e privacidade no âmbito do acesso, manipulação, tratamento e disponibilização dos dados de professores e alunos proporcionados pelos Ambientes Virtuais de Aprendizagem (AVA).

2.1 Objetivos específicos:

- Apontar as formas de segurança e privacidade no acesso de dados;
- Caracterizar as formas de disponibilização e tratamento de dados, contextualizando com a legislação brasileira;
- Ressaltar a importância da privacidade e segurança na manipulação de dados criados ou decorrentes das pesquisas online, considerando, sobretudo, a questão dos impactos criados e suas influências na questão da discriminação e preconceitos.

3. Desenvolvimento

3.1 Acesso de dados:

Em relação ao controle de acesso dos dados deve-se atentar para questões normativas e padronização de condutas, assim, a norma ABNT NBR ISO/IEC 27002:2013, denominada de: “Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação”, aborda no capítulo 9 o acesso de dados, que especificamente contribui na aplicação e na definição de uma política de controle de acesso. Esta norma reforça que o acesso à informação deve ser controlado e o sistema deve ser capaz de possibilitar o acesso aos usuários autorizados e impedir o acesso de pessoas não autorizadas, com o intuito de prevenir danos aos sistemas de informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013).

Na Figura 1 observam-se as categorias de controle de acesso, com as ramificações nos requisitos do negócio para controle do acesso, gerenciamento de acesso do usuário, responsabilidades dos usuários e controle de acesso ao sistema e a aplicação, detalhando os objetivos e ações necessárias para execução.

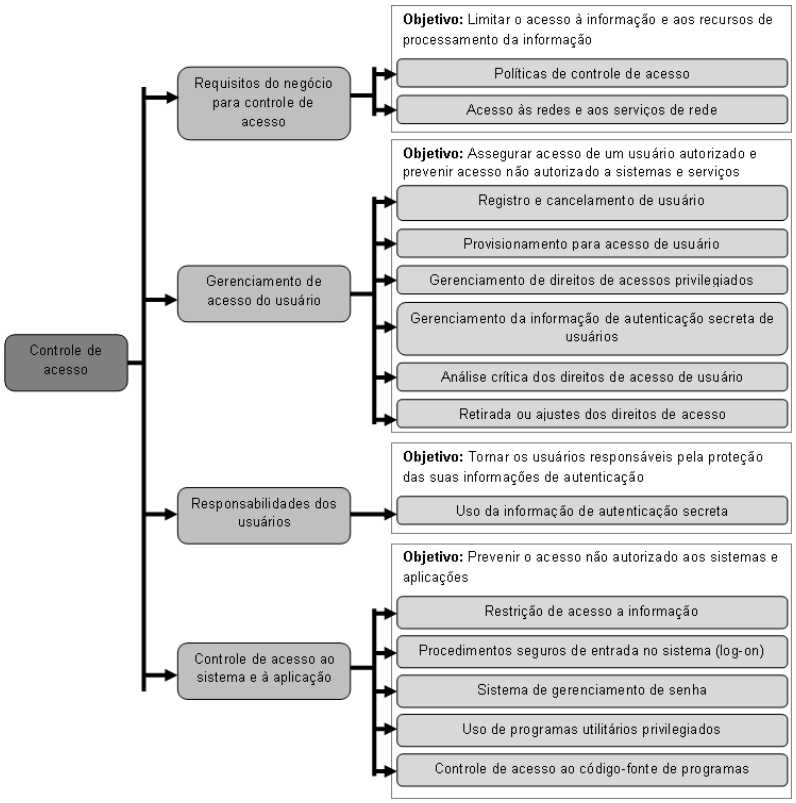

Figura 1: Categorias de controle de segurança.

Adaptado de: [Coelho & Araújo, 2014].

Para cada objetivo, apresentado na figura 1, temos recomendações descritas abaixo.

Quanto a Requisitos do negócio para controle de acesso:

A. Políticas de controle de acesso: Deve-se se estabelecer, documentar e analisar criticamente a política de controle de acesso, baseada nos requisitos de segurança da informação e dos negócios.

B. Acesso às redes e aos serviços de rede: Os usuários devem ter acesso apenas às redes e serviços que foram autorizados.

Quanto ao gerenciamento de acesso do usuário:

A. Registro e cancelamento de usuário: Recomenda-se um processo formal de registro e cancelamento de usuário para permitir os direitos de acesso.

B. Provisionamento para acesso de usuário: Implementação de um processo formal de provisionamento de acesso do usuário para conceder ou revogar os direitos de acesso em todos os tipos de sistemas e serviços.

C. Gerenciamento de direitos de acesso privilegiados: A concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados.

D. Gerenciamento da informação de autenticação secreta de usuários: Uso de autenticação secreta controlada por um processo formal.

E. Análise crítica dos direitos de acesso de usuário: Em tempos regulares, seja realiza a análise crítica dos direitos de acesso dos usuários pelos proprietários.

F. Retirada ou ajustes dos direitos de acesso: Recomenda-se que após o encerramento de atividades, acordos ou contratos os direitos de acessos sejam ajustados ou revistos.

Quanto a responsabilidades dos usuários:

A. Uso da informação de autenticação secreta: Os usuários devem receber orientações sobre o uso da informação com autenticação secreta.

Quanto ao controle de acesso ao sistema e à aplicação:

A. Restrição de acesso à informação: A restrição deve estar de acordo com a política de controle de acesso.

B. Procedimentos seguros de entrada no sistema (*log-on*): Os acessos aos sistemas e aplicações devem ser controlados por um procedimento de entrada (log-on)

C. Sistema de gerenciamento de senha: Sejam interativos e assegurem senhas de qualidade.

D. Uso de programas utilitários privilegiados: Possam ser capazes de sobrepor os controles dos sistemas e aplicações e sejam restritos e estritamente controlados.

E. Controle de acesso ao código-fonte de programas: Recomenda-se que seja restrito. (ABNT, 2013).

Ressalta-se que as normas da ABNT são elaboradas por Comissões de Estudos com membros dos setores envolvidos, sendo eles, produtores, consumidores e neutros (universidades, laboratórios e outros) (ASSOCIAÇÃO BRASILEIRA DE NOMAS TÉCNICAS, 2013)

No mercado existem várias empresas trabalhando com controle de acesso de dados, um exemplo é a Salesforce Platform, empresa de assessoria, que oferece serviços para controle de acesso de dados, que podem ser utilizados em várias situações. Essa empresa refere que o controle de dados possibilita a facilidade de acesso, e possibilita ao usuário a exibição, criação, edição, ou exclusão de um registro em seus aplicativos. A empresa oferece como exemplo de aplicativo um controle de acesso de dados de recrutamento, possibilitando o gerenciamento das vagas em aberto, candidatos e formulários de emprego (TRAILHEAD, 2020).

A figura 2 ilustra o contexto de controle de acessos, como ferramenta de Inteligência Artificial (IA).

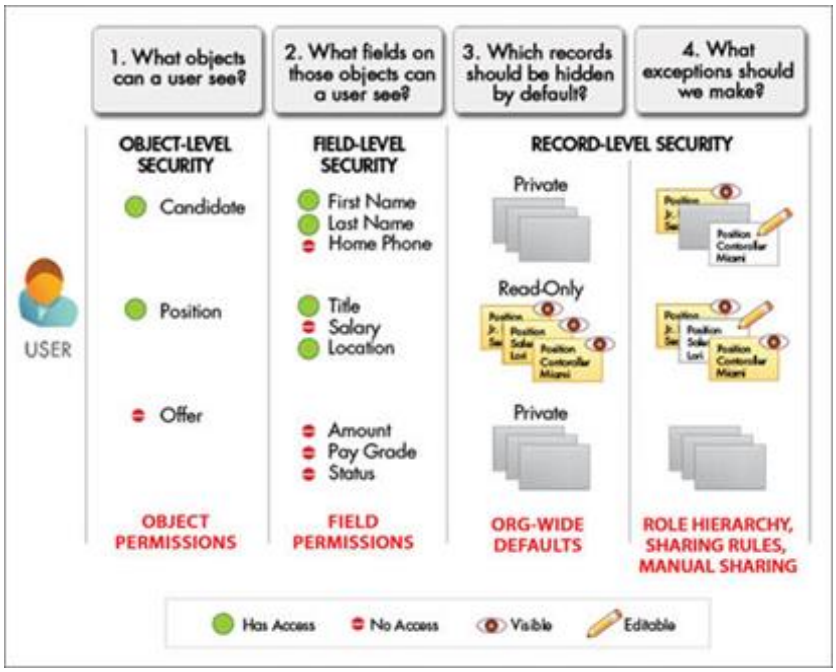

Figura 2: Controle de acesso de dados.

Fonte: [Trailheal, 2020].

Assim, observa-se na figura 2 que quando se cria um aplicativo ou plataforma são importantes os itens: Quais objetos/assuntos um usuário/utilizador pode ver, a segurança no nível do objeto e ainda, a permissão para acesso aquele objeto/assunto; Quais campos nesses objetos/assuntos um usuário pode ver, a segurança em nível de campo e o campo de permissão; Quais registros devem estar ocultos por padrão, a segurança de nível de registro e os padrões gerais da organização; Que exceções fazemos, a segurança de nível de registro e a hierarquia de papéis/regras de compartilhamento manual.

Logo, segundo a Trailhead (2020) é possível ter o controle de acesso de toda uma instituição desde que se estabeleça uma combinação de controle por níveis e especificando as permissões de todos os usuários aos dados.

Quando a realidade de acesso de dados é transposta para a área da Educação, no momento atual da obrigatoriedade do trabalho remoto, grande parte dos docentes não

estava pronto para o uso desses recursos remotos, embora tivessem acessibilidade a eles (ANGELUCCI, 2017).

Segundo Tokarnia (2019), uma porcentagem menor que 50% dos estudantes têm aprendido sobre as questões de segurança no acesso e uso da internet.

Na questão do número de alunos, que são efetivamente assessorados pelos seus professores, e conforme estudos e apontamentos do Comitê Gestor da Internet (CGI), somente 44 % dos estudantes de escolas públicas foram orientados pelos seus professores sobre o uso da internet de uma forma segura, além disso, 78 %, tem feito seus acessos de forma pessoal, com objetivos de buscar dados sobre tecnologias. Esses acessos têm sido viabilizados por meio da utilização de vídeos e tutoriais explicativos, de forma que essas ferramentas possam conduzi-los a essas pesquisas. Outra estratégia que os alunos utilizam é a consulta a parentes ou amigos (76%). Ressalta-se que 38% dos docentes declararam já ter ajudado os alunos diante de situações como: bullying, discriminação, assédio e propagação de imagens sem consentimento durante o acesso à internet (TOKARNIA, 2019).

Com a alteração da Lei nº 12.730, de 11/10/2007, que proibia o uso de celulares em salas de aula, que foi substituída pela Lei número 16.567, de 06/11/2017, mudando a redação do artigo 1º da Lei nº 12.730, que passou a vigorar com a seguinte redação: "Artigo 1º- Ficam os alunos proibidos de utilizar telefone celular nos estabelecimentos de ensino do Estado, durante o horário das aulas, ressalvado o uso para finalidades pedagógicas.". Logo, os celulares passam a ser uma ferramenta de captação de dados de alunos e professores (ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO, 2017).

Nas questões específicas da educação, às instituições de ensino devem considerar as questões éticas, decorrentes dos dados que mantêm dos seus alunos e das

formas de acesso, devendo privilegiar, sobretudo, a melhoria na diminuição dos índices de retenção e com foco principal no sucesso acadêmico do aluno (SCLATER, 2014).

Assim, diante do atual ensino remoto as instituições devem estar atentas ao controle de acesso de dados nas plataformas ou meios de comunicação para que alunos e professores não sejam expostos ou tenham seus dados disponibilizados, manipulados ou tratados com objetivos de marketing, ou outras finalidades.

3.2 Disponibilização de dados

Durante qualquer acesso à internet**,** seja por meio de aplicativos ou simplesmente quando se utiliza uma ferramenta de busca, os sistemas operacionais transformam as informações em dados, e esses dados são disponibilizados de acordo com os termos de uso e privacidade de cada plataforma. Logo, o principal desafio é preservar os dados disponibilizados desde a criação de uma conta de e-mail, onde são fornecidos os dados pessoais para as empresas de tecnologias que, após este momento, inicia a coleta de dados para a utilização de melhoras e desenvolvimento de novos produtos de acordo com as preferências dos usuários (SENIOR, 2020).

Analisando os Termos de Uso e Privacidade das redes sociais mais utilizadas e dos serviços G Suíte do Google® (2020), fica claro os dados que são coletados e como são utilizados por estas empresas. Os principais dados coletados são:

- Dados da conta;
- Mensagens enviadas e recebidas;
- Contatos estabelecidos e salvo na agenda;
- Uso e dados de registro;
- Dados de transações;
- Dados sobre dispositivos e conexões;
- Cookies;

- Dados de status;
- Prestadores de serviço terceirizados;
- Histórico de navegação nos produtos da família da plataforma;
- Dados de localização;
- Atividades no site ou em sites de terceiro.

Mediante a disponibilização desses dados pode-se refletir em relação aos aspectos de segurança, privacidade e ética na internet e como essas informações ajudam estes serviços a operar, entender, aprimorar, dar suporte, personalizar e a promover serviços de prestadores de serviços on-line.

Assim, mediante as circunstâncias ocorridas pela pandemia do COVID-19, especialmente, com o isolamento social e fechamento das unidades educacionais pelas autoridades, o Ministério da Educação (MEC) publicou a Portaria nº 345, de 19 de março de 2020, autoriza que as aulas presenciais sejam substituídas por aulas que utilizam meios digitais enquanto durar a pandemia. (BRASIL, 2020).

Frente a isso, iniciou-se a utilização de diferentes plataformas e redes sociais para a interação de professores e estudantes em todas as etapas da educação, gerando diferentes e milhões de dados a cada minuto para as companhias responsáveis por esses domínios digitais.

Dentro deste contexto, onde estão sendo gerados dados a todo instante, pergunta-se: Os dados educacionais são disponibilizados com privacidade e segurança? As pessoas sabem como e para quê estes dados estão sendo disponibilizados?

Com o avanço do isolamento social, a educação remota emergencial ganhou força com a utilização de vários ambientes de aprendizagem virtual. Em recente reportagem publicada no jornal Folha de São Paulo, em 27 de abril de 2020, relata que o acesso a plataforma Zoom ultrapassou de 10 milhões de usuários/dia para 300 milhões de

usuários/dia. A reportagem informa que durante o acesso dos participantes de reuniões educacionais outros usuários adentravam as salas virtuais e iniciavam atividades e uso de palavras inadequadas que atrapalhavam as aulas remotas. Além, das invasões, ocorreu a divulgação de conteúdos atribuídos aos participantes que não o fizeram e a disponibilização de dados para outras plataformas com fins comerciais (SOPRANA, 2020).

Apesar de essas plataformas utilizarem de criptografias como está descrito em seus Termos de Privacidade para a segurança e privacidade de seus usuários, os dados podem ser descriptografados e utilizados pelos seus desenvolvedores para outras finalidades (ZOOM,2020; WHATSAPP,2020).

Deve-se ressaltar que além das mensagens, número de acessos, dados como da agenda pessoal e de outras pessoas em grupos de mensagens ficam disponíveis e tem-se uma geração de dados exponencial, ou seja, um usuário único, gera dados de milhares de usuários que estão em seu convívio digital. Logo, professores que atualmente disponibilizam dados de suas turmas, atividades realizadas e programadas, dados de outros colegas professores e de pais ou responsáveis pelos estudantes ficam expostos a falta de segurança, privacidade e ética no meio digital. (WHATSAPP, 2020).

Neste sentido, temos a Lei Geral de Proteção de Dado, Lei nº 13.709, de 14 de agosto de 2018, muito recente, e que foi promulgada e entrará em vigor em agosto de 2020, a qual prevê a proteção de dados por meio da privacidade dos dados pessoais, autodeterminação informativa, liberdade de expressão, de informação, comunicação e de opinião entre outros fundamentos. Essa legislação promoverá uma redução na disponibilização de dados, pois será necessário o consentimento dos usuários para que os dados sejam utilizados com segurança e ética, contudo em uma época onde existe a

necessidade de múltiplos acessos em diferentes plataformas, os dados disponibilizados tornam-se produtos para serem utilizados como motivo de recomendações de acesso e produtos (BRASIL, 2018).

Além da disponibilização dos dados nas plataformas, vale a reflexão dos impactos das redes sociais que disponibilizam muitos dados na sociedade. Com a utilização dos serviços de mensagem para a resolução de problemas e desenvolver comunicação, a sociedade deve ter a atenção se o processamento desses dados não repliquem discriminação e preconceito.

Portanto, é fundamental destacar que os dados disponibilizados atualmente na educação remota emergencial podem estar sendo utilizados para desenvolverem e/ou alimentar sistemas de Inteligência Artificial com base nas plataformas e redes sociais destinadas a essa modalidade de ensino e a sociedade terá que estar atenta nos quesitos da ética, segurança e privacidade compartilhadas pelas tecnologias digitais.

3.3 Manipulação de dados

A segurança da informação é baseada em três princípios básicos, que são considerados como seu alicerce e, portanto, imutáveis e imprescindíveis, são eles: confidencialidade, integridade e disponibilidade. Além desses princípios considerados como seu alicerce, outros atributos são destacados: autenticidade, não-repúdio e conformidade (COELHO, 2013). Abaixo a descrição dos atributos (Tabela 1):

Tabela 1: Atributos da segurança da informação.

Atributo	Característica ou função
Confidencialidade	Garantir acesso somente de pessoas autorizadas.
Integridade	Assegurar e prevenir modificações não autorizadas.
Disponibilidade	Prover acessibilidade e utilização sob demanda.
Autenticidade	Propriedade de uma entidade ser o que afirma que é.
Não-repúdio	Provar ocorrência de suposto evento ou ação.
Conformidade	Assegurar processos em conformidade com a legislação.

Fonte: [Adaptado de (HINTZBERGEN, 2018)]

Com o objetivo de cumprir com seus princípios básicos, a segurança da informação conta com alguns recursos, sendo estes, normalmente classificados como: recursos físicos, recursos lógicos e recursos humanos. Os recursos físicos são as instalações e proteções, a fim de que os dados não sejam danificados, por exemplo, por uma pane elétrica. Com relação aos recursos lógicos, podemos considerar as constantes atualizações de sistemas, o estabelecimento de padrão na geração de senhas, a auditoria em contas de e-mails e políticas de restrição de acesso a determinados sites. Já o recurso humano, que envolve toda e qualquer interação com a informação, é o elemento fundamental e talvez o mais importante, uma vez que as pessoas estão diretamente envolvidas com processos que se relacionam com a informação, e desta forma, tende a ser o elo mais fraco da segurança da informação (SILVA, 2015).

Tal fragilidade está relacionada diretamente com o princípio da integridade, que visa evitar o ataque que se dá por meio de manipulações (adições, remoções ou alterações) não autorizadas. A Figura 3, ilustra o fluxo normal e o fluxo do modelo de ataque por manipulação.

Figura 3: Modelo de ataque de manipulação.

Fonte: Adaptado de [COELHO, 2013]

Uma forma de manipulação considerada comum ocorre por meio da apresentação gráfica dos dados, na figura 4, observam-se dois gráficos com os mesmo valores, mas

com apresentações diferenciadas. Nota-se que ocorre uma manipulação na escala de variação do eixo Y (Score), nos Resultados A tem-se a variação de 20 unidades e no gráfico de Resultados B a variação é de uma unidade. Dessa forma, a curva dos dados se apresenta em formatos diferenciados e essa manipulação pode influenciar e impactar na interpretação dos dados (DATA ETHICS, 2010).

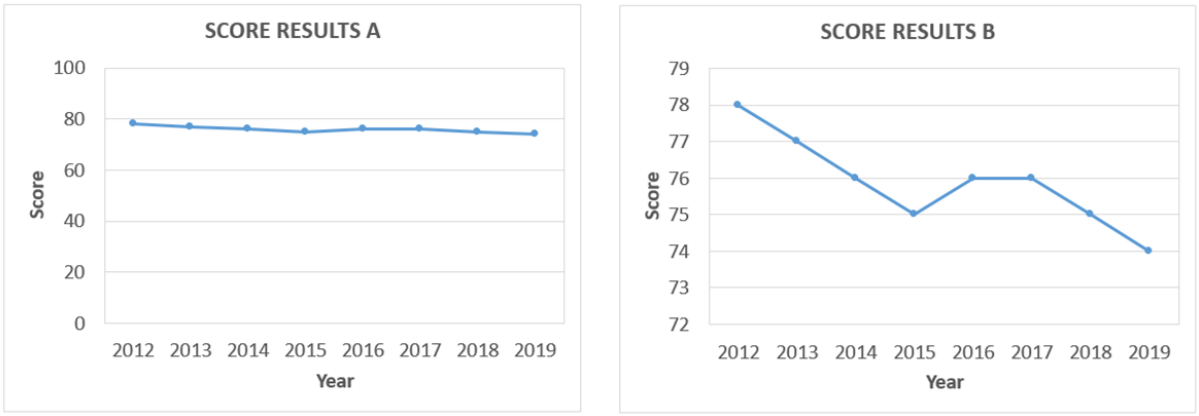

Figura 4: A manipulação pode influenciar uma interpretação.

Fonte: Adaptado de [DATA ETHICS, 2010]

Em 2019 com o lançamento do documentário Privacidade Hackeada, inspirado em fatos reais, exemplifica-se outra forma de manipulação de dados provenientes do Facebook e que pode influenciar o comportamento e a vida das pessoas. O documentário enfatiza como os cidadãos que utilizam a rede social não percebem que são expostos ao consumismo e que as informações relativas ao seu perfil podem ser utilizadas inclusive no campo da política, manipulando eleitores mais suscetíveis e induzi-los na opção de escolha de um determinado candidato.

Ainda no documentário é exposta a empresa Cambridge Analityca que se utilizou dos dados de perfis dos usuários do Facebook para o processo eleitoral nos Estados Unidos. Nesse contexto, um dos candidatos foi eleito com auxílio do uso estratégico e manipulação das pessoas. Os proprietários e envolvidos no processo de manipulação dos dados enriqueceram de forma ilícita e a empresa decretou o encerramento de suas

atividades após a descoberta e investigação da análise e manipulação de dados (PRIVACIDADE HACKEADA, 2019).

Um outro exemplo, mas agora relacionado a manipulação por "sequestro" de informação, foi constatado recentemente na plataforma de videoconferência Zoom®, que em tempos de pandemia e por conta da necessidade da realização de aulas remotas ou reuniões corporativas, viu seu número de usuários crescer em aproximadamente 1900%. O ocorrido foi que muitos usuários tiveram suas chamadas "sequestradas" por usuários não autorizados. O incidente se baseava em, durante uma aula ou reunião, apareciam pessoas não autorizadas e começavam a transmitir conteúdos ofensivos ou pornográficos (FBI, 2020).

Os recursos de IA, no que se refere ao uso das redes sociais, possibilitam a busca de informações e a obtenção de dados de uma forma ilimitada, sem conhecimento e consciência desse contexto manipulativo. Esse uso indevido, sem consentimento, ultrapassa os limites da questão ética. Espera-se que com a legislação recentemente criada LGPD, inspirada no Regulamento Geral de Proteção de Dados (GDPR), da União Europeia, os atributos citados acima anteriormente sejam respeitados no Brasil (Tabela 1).

Outra questão a ser considerada é com relação a manipulação de grandes volumes dados, armazenadas em estruturas conhecidas como Big data (um termo guarda-chuva, que de forma bem resumida, diz respeito a um conjunto de técnicas utilizadas para realizar análises de grandes volumes de dados), que são os dados individuais coletados, quando do acesso à internet, por exemplo, para uso em estâncias indevidas e sobretudo sem o consentimento dos cidadãos e que, segundo Sclater (2014), necessita-se o estabelecimento de princípios e melhores práticas das partes interessadas, de forma a manter a privacidade.

Com base no exposto, não há, pelo menos ainda, uma forma de se garantir quem está do outro lado de um sistema informatizado, realizando ou concluindo uma atividade ou mesmo uma avaliação, o que torna difícil garantir a segurança e veracidade das informações que estão sendo geradas, podendo estas, estarem sendo manipuladas, através por exemplo, do simples ato de copiar e colar conteúdos. Somado a isso, possíveis falhas de segurança física e lógica, podem agravar ainda mais o cenário onde se deseja manter a ética, privacidade e segurança da informação dado que o volume de dados será cada vez maior. Assim, mesmo com as precauções e investimentos como: utilização de biometria, sistemas com alto nível de criptografia a fim de se evitar ou blindar cópias (REIS, 2010), disponibilização de estruturas de hardware e softwares compatíveis com as necessidades dos usuários, profissionais capacitados e treinamento para melhor utilização e manutenção desses recursos, de forma a atender a todos os requisitos básicos da segurança da informação, é preciso contar com a ética e, para isso, considerar o fator humano, que, como mencionado anteriormente, tende a ser o elo mais fraco dessa corrente.

Dessa forma, a construção de um ambiente que garanta a segurança dos dados, requer conscientização, ações e envolvimento de todos, inclusive com planejamento detalhado, desde a categorização das informações, com relação a sua criticidade (se alta, média ou baixa), de acordo com uma classificação interna, e os possíveis impactos, em caso de vazamento desses dados. Assim, a integridade, no que diz respeito a manipulação, deve ser realizada somente por pessoas autorizadas, com discrição e ética, sem causar prejuízo a informação.

Portanto, deve haver um comprometimento com a capacitação constante não só da administração das escolas, mas também do corpo docente, demais possíveis colaboradores e discentes no uso ético, seguro e legal das Tecnologias da Informação e Comunicação - TIC's, bem como das informações por elas produzidas.

3.4 Tratamento dos dados

As tecnologias estão em constante atualização e acabam por assumir novas participações na vida da humanidade, assim como trás comodidades e facilidades, também gera preocupações quanto ao uso e quanto à exposição da sociedade, e com a IA isso não é diferente. A preocupação mais frequente é se o ser humano poderá ser substituído por máquinas, tanto no ambiente industrial como no escolar, mas será que este é o único ou maior problema? (RODDRIGUES,2018).

Uma questão muito discutida nos últimos tempos é o tratamento dos dados adquiridos para que a inteligência artificial tome suas decisões, pois esta é uma tecnologia voltada ao aprendizado, e como esta máquina está aprendendo? A aquisição destes dados deve ser utilizada de forma que não se forme tendências discriminatórias e preconceituosas, mas se a máquina aprende com o homem e essas tendências fazem parte da sociedade, como evitar que isso ocorra? (CORTIZ, 2020).

O uso da IA com viés discriminatório tem sido estudado atualmente (CORTIZ, 2020), e um exemplo recente, foi em 2016, com o estudo da ProPublica que mostrou o sistema de justiça dos EUA, atribuindo graus de risco de reincidência em crimes, para réus negros e brancos, com maiores riscos para os réus negros (Figura 7), independente se isso tenha sido realmente verificado na forma prática (BIAS MACHINE,2016).

Figura 5 – Pontuação de risco atribuídas a réus negros e brancos

Fonte: [MACHINE BIAS,2016]

Até mesmo empresas sérias que procuram combater o tratamento de dados com cunho discriminatório acabam sendo surpreendidas com seus algoritmos de sistemas de IA (TEIXEIRA, 2019), por exemplo, a Amazon ao analisar seu sistema de IA para recrutamento de candidatos percebeu que este favorecia a seleção de candidatos do sexo masculino. Esse favorecimento com resultados de análise de algoritmos de seleção de candidatos que associam a mulher à família e o homem ao trabalho foi pauta da Revista Veja em 2017, com vários exemplos de como o tratamento dos dados pode contribuir para a discriminação.

Como então utilizar a inteligência artificial na educação e ser imparcial, se isso é um dos problemas que já ocorrem na sala de aula (SILVA E MAMEDIO, 2016), é papel fundamental entender quais são as motivações e desmotivações de alunos e professores e como a relação entre eles impactam no processo de ensino e aprendizagem.

Pensando nos aspectos éticos relacionados ao tratamento de dados é necessário refletir quanto ao uso de forma ética no desenvolvimento da IA, para isso, a Declaração de Montreal para a Responsabilidade e Desenvolvimento da Inteligência Artificial (2018), elaborada por uma equipe multidisciplinar, propõe diretrizes para a utilização de forma ética da IA e onde são defendidos dez princípios de igual importância, listados abaixo:

- Princípio do Bem Estar;
- Princípio do respeito à Autonomia;
- Princípio de proteção da privacidade e intimidade das Pessoas;
- Princípio da solidariedade;
- Princípio da participação democrática;

- Princípio da igualdade;
- Princípio da inclusão e diversidade;
- Princípio da prudência;
- Princípio de responsabilidade;
- Princípio de desenvolvimento sustentável.

Esses princípios de tratamento de dados em sistemas de inteligência artificial devem ser aplicados inclusive quando utilizado esse tipo de tecnologia no âmbito educacional, garantindo assim, imparcialidade e justiça nas tomadas de decisões (UNIVERSIDADE DE MONTREAL, 2018).

Quando pensa-se em princípio do respeito à Autonomia, busca-se formar o indivíduo crítico para protagonizar a construção de conhecimentos no seu processo educacional (ANDRADE e SOUZA, 2013), além disso refletir para que os sistemas de IA não impeçam o indivíduo de seguir sua própria moral e valores, e que a formação seja para a aquisição de habilidades, conhecimentos e uso crítico das tecnologias que existem, para que não contribuam para a disseminação de informações não confiáveis ou fake news.

No Princípio da Participação Democrática no tratamento de dados o sistema deve mostrar com clareza as tomadas de decisões aos usuários, como os dados foram utilizados em toda a aplicação, para que possibilite consciência e transparência, além de promover a interação, aceitação desta tecnologia e auxiliar no entendimento de como funciona (UNIVERSIDADE DE MONTREAL, 2018). Esses princípios confirmam a necessidade da escola preparar os alunos para a democracia, educando-os para a realidade preservando a liberdade de pensamento e decisão (BASTOS, 2017).

Como apresentado anteriormente a IA aprende com a sociedade, e o preconceito é uma realidade, assim os dados e a forma de tratamento devem ser trazer benefícios aos

alunos e não serem utilizados para classificá-los de forma isolada, pensando nisso surgem os princípios da Igualdade e da Inclusão e Diversidade com o objetivo que o tratamento de dados não exclua as pessoas considerando sua raça, cor, etnia, gênero ou cultura e que possibilite as relações de poder de determinados grupos sobre outros. Este é um dos maiores desafios desta tecnologia, pois os sistemas de IA são alimentados por programadores que podem inconscientemente agregar seus valores e princípios aprendidos e isso resultar no aumento das desigualdades (UNIVERSIDADE DE MONTREAL, 2018).

A utilização de dados para alimentar sistemas inteligentes na educação já se faz presente em algumas instituições educacionais com o uso de plataformas, que possibilitam o gerenciamento da vida acadêmica do aluno, por meio de atividades realizadas na plataforma e pelos dados pessoais e sociais, possibilitando assim prever a evasão escolar do aluno considerando não apenas sua vida acadêmica, mas correlacionando com sua participação na sociedade e seus dados socioeconômicos (RIGO et al, 2014). São questionados se somente esses dados são capazes de realmente, e de forma justa, entender a situação do aluno sem que ocorra a quebra da privacidade do indivíduo, e até que ponto pode-se fazer o uso de dados pessoais em um sistema inteligente?

Assim, o Decreto de Montreal, traz o Princípio de Proteção da Privacidade e Intimidade das Pessoas, onde é previsto espaços predeterminados para a inserção dos dados sem qualquer tipo de vigilância, essa medida contribui para a preservação da intimidade de pensamentos, evita a discriminação e julgamentos sobre as escolhas do usuário.

Logo, no ambiente educacional os dados acadêmicos e pessoais do aluno devem ser tratados com sigilo, já que podem ser utilizados de forma dolosa por terceiros, expondo o educando ao constrangimento e discriminação. (RIGO et al, 2014).

O Princípio da Prudência reforça a necessidade de criação de mecanismos que identifiquem usos inadequados dos dados ou barreiras para proteção de invasões externas. (UNIVERSIDADE DE MONTREAL, 2018). Assim, as plataformas de ensino com IA devem ser elaboradas com sistemas de proteção de dados robustos que possibilitem a identificação de potencial invasão e/ou identificação de formas inapropriadas de utilização, devem contar com ferramentas de bloqueio e de denúncias aos responsáveis mediante essas situações.

É de extrema importância que o educador e educando tenham ciência dos dados disponibilizados e quais suas utilizações. Além de terem o conhecimento de como proceder quando houver a necessidade de proteção de direitos autorais e de imagem, assim como em todos os outros princípios, a transparência quanto ao tratamento dos dados e sua segurança deve estar sempre presente, haja visto que, as tecnologias educacionais estão cada vez mais ganhando espaço e a preocupação com a segurança dos dados é fundamental (BORELLI, 2019).

A pandemia do COVID-19 trouxe um novo cenário para a educação mundial, aproximadamente 1,2 bilhões de alunos foram afetados pelo fechamento de escolas em todo o mundo (UNESCO,2020), e os professores precisaram produzir material e disponibilizá-los na internet sem qualquer preparo ou planejamento (GIFE, 2020) .

Com esse aumento dos dados, enviados pelas plataformas educacionais e redes sociais, constata-se a exposição de dados de professores e alunos no Brasil. No entanto, indo na contramão da segurança no tratamento de dados, o governo brasileiro prorroga a implementação da Lei lei 13.709/18, a Lei Geral de Proteção de Dados (LGPD) por meio

da medida provisória nº. 954, tendo como resultado, o país sem legislação de proteção de dados. Tal medida é justificada pelo poder público como forma de não onerar as empresas economicamente nesse momento com a implantação da Legislação. No entanto, alguns autores colocam que a medida tem a intenção de preservar a judicialização em massa da população em relação ao uso dos dados, além de possibilitar e permitir o uso dos dados de geolocalização para o controle do isolamento social da população brasileira e auxiliar no controle do contágio do vírus. (SILVEIRA E PORTELLA, 2020).

Diante de um cenário tão desafiador os dados de professores e alunos estão atrelados apenas às políticas de segurança e privacidade dos aplicativos e ferramentas e estarão à mercê de crimes cibernéticos e possíveis manipulações e tratamento de dados.

4. Conclusão:

A pandemia do Covid-19 trouxe para o mundo e principalmente para o Brasil um momento de reflexão e oportunidade para trazer a Educação Online para o cotidiano dos professores e alunos, no entanto, os princípios de ética, segurança e privacidade ainda estão frágeis e vulneráveis, assim como o acesso, disponibilização, manipulação e tratamento de dados estão susceptíveis ao cibercrime e usos inapropriados.

A ausência de uma legislação vigente oferece a possibilidade de que pessoas más intencionadas aproveitem para captar dados e utilizar para outras finalidades, que não seja a educação.

Serão necessários estudos para constatar se os princípios da ética, segurança e privacidade têm sido respeitados e como os dados estão sendo tratados nesse novo cenário.

5. Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISSO/IEC 27002. Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. 2013.

ANDRADE, L.; SOUZA, T. N. **Fundamentos da Educação Infantil**. Batatais: Claretiano, 2013.

ANGELUCCI, B. **Muito além das tarefas a cumprir: notas da FEUSP sobre a educação em tempos de isolamento.** Faculdade de Educação da Universidade Estadual de São Paulo. São Paulo, 2020. Disponível em: http://www4.fe.usp.br/wp-content/uploads/documento-fe-em-tempos-de-isolamento.pdf. Acesso em: 4 de maio de 2020.

ASSEMBLÉIA LEGISLATIVA DO ESTADO DE SÃO PAULO. Lei nº 16.567, de 06 de novembro de 2017. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/lei/2017/lei-16567-06.11.2017.html. Acesso em: 4 de maio de 2020.

BASTOS, M.J. **A Importância da Ética na Educação. Revista Científica Multidisciplinar Núcleo do Conhecimento.** Edição 05. Ano 02, Vol. 01. p 264-276, Julho de 2017.

BORELLI, A. **LGPD – Como os colégios se preparam para segurança das plataformas utilizadas por alunos e professores.** São Paulo, 2020. Disponível em: https://cryptoid.com.br/protecao-de-dados/lgpd-como-os-colegios-se-preparam-para-seguranca-das-plataformas-utilizadas-por-alunos-e-professores/. Acesso em: 05 de maio de 2020.

BOTO, C. **A educação e a escola em tempos de coronavírus.** Jornal da Universidade Estadual de São Paulo, 2020. Disponível em: https://jornal.usp.br/artigos/a-educacao-e-a-escola-em-tempos-de-coronavirus/. Acesso em: 04 de maio de 2020.

BRASIL. Lei Geral de Proteção dos dados. Lei n 13709 de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 de maio de 2020.

BRASIL. Ministério da Educação. Decreto 9.057 que regulamenta o art. 80 da Lei nº 9.394, de 20 de dezembro de 1996 e estabelece as diretrizes e bases da educação nacional. Disponível em: http://portal.mec.gov.br/escola-de-gestores-da-educacao-basica/355-perguntas-frequentes-911936531/educacao-a-distancia-1651636927/12823-o-que-e-educacao-a-distancia e http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9057.htm#art24. Acesso em: 05 de maio de 2020.

BRASIL. Ministério da Educação. Portaria n345, de 19 de março de 2020. Substituição das aulas presenciais por aulas em meios digitais enquanto durar a situação de pandemia do Novo Coronavírus – COVID-19. Disponível em: https://www.semesp.org.br/wp-content/uploads/2020/03/PORTARIA-N%C2%BA-345-DE-19-DE-MAR%C3%87O-DE-2020.pdf. Acesso em: 06 de maio de 2020.

BRASIL. RESOLUÇÃO Nº 466, DE 12 DE DEZEMBRO DE 2012. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/cns/2013/res0466_12_12_2012.html**.** Acesso em 07 de maio de 2020.

BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em : http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 05 de maio de 2020.

COELHO, F.E.S.; ARAUJO, L.G.S. **Gestão da Segurança da Informação – NBR 27001 e 27002**. Rio de Janeiro: Escola Superior de Redes, RNP, 2014. Disponível em: <file:///C:/Users/dell/Downloads/kupdf.net_gestao-da-segurana-da-informaao-nbr-27001-e-nbr-27002.pdf>. Acesso em 25 de maio de 2020.

CORTIZ, D. Viés, preconceito, discriminação na inteligência artificial, 2020. Disponível em: https://medium.com/@diogocortiz/vi%C3%A9s-preconceito-discrimina%C3%A7%C3%A3o-na-intelig%C3%AAncia-artificial-6d1f05c33e5a. Acesso em: 05 de maio de 2020.

DATA ETHICS. **The Forum Guide to Data Ethics**. NCES - The National Center for Education Statistics, 2010.. Disponível em: https://nces.ed.gov/pubs2010/2010801.pdf. Acesso em: 10 de maio de 2020.

FBI. **Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic**. 2020. Disponível em: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic. Acesso em: 26 de maio de 2020.

GIFE. **Planejamento, conectividade e tecnologia: quais são os principais desafios da educação em tempos de pandemia**, 2020. Disponível em:https://gife.org.br/planejamento-conectividade-e-tecnologia-quais-sao-os-principais-desafios-da-educacao-em-tempos-de-pandemia/. Acesso em: 26 de maio de 2020.

GOOGLE FOR EDUCATION. **Contrato do G Suite for Education,** 2020. Disponível em: https://gsuite.google.com.br/intl/pt-BR/terms/education_terms.html. Acesso em 06 de maio de 2020.

HINTZBERGENN, J.; HINTZBERGENN, K; BAARS H; SMULDERS A. **Fundamentos da Segurança da Informação: com base na ISO 27001 e na ISO 27002.** Editora Brasport, 2018.

HODGES, C.; MOORE, S; LOCKEE, B; TRUST, T; BOND, A. **The Difference Between Emergency Remote Teaching and Online Learning.** Educause Review, 2020. Disponível em: https://er.educause.edu/articles/2020/3/the-difference-between-emergency-remote-teaching-and-online-learning. Acesso em: 05 de maio de 2020.

VEJA. **Inteligência Artificial apresenta traços racistas e machistas: Novo estudo identificou que nomes femininos são associados por computadores à família, enquanto os masculinos, à**

profissão. São Paulo, Brasil, 16 abr. 2017. Disponível em: https://veja.abril.com.br/ciencia/inteligencia-artificial-apresenta-tracos-racistas-e-machistas/. Acesso em: 5 abr. 2020.

JUNQUEIRA, E.S. **Vigilância em Tempos de Educação à Distância**. Outras Palavras. Jornalismo de Profundidade e pós capitalismo, 2020. Disponível em: https://outraspalavras.net/tecnologiaemdisputa/vigilancia-em-tempos-de-educacao-a-distancia/. Acesso em: 05 de maio de 2020.

LIMA, J.M.C.; MARTINS JR, F.R.F; NOBRE, R.H.; DIAS, N.M.F. **Informática na sociedade e ética**. Ed. UECE. Fortaleza, 2016.73p.

MACHINE BIAS. **There's software used across the country to predict future criminals. And it's biased against blacks**, 2016. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em:05 de maio de 2020.

MORAN, J.M. **Contribuições para uma pedagogia de educação online.** In: Educação online: teorias, práticas, legislação, formação corporativa.2ed. Ed. Loyola, São Paulo, 2003.

PEDRO, A.P. **Ética, moral, axiologia e valores: confusões e ambiguidades em torno de um conceito comum**. Kriterion: Revista de Filosofia. Belo Horizonte, nº 130, Dez./2014, p. 483-498. doi: https://doi.org/10.1590/S0100-512X2014000200002

PRIVACIDADE RACKEADA. Direção: Amer K, Noujaim J. Estados Unidos: NETFLIX, 2019. Disponível em: Netflix. Acesso em: 5 abr. 2020.

REIS, H.T.E. **Segurança da informação e a Educação à distância**, 2010. Disponível em: http://www.periodicos.letras.ufmg.br/index.php/ueadsl/article/view/2688. Acesso em: 11 de maio de 2020.

RENAUD, I. **A noção de dever na ética contemporânea**. In: J. Brito (Coord.). Temas fundamentais de ética (pp. 31-44). Braga: Universidade Católica Portuguesa, 2001.

RIGO, S. J.; BARBOSA, J.; CAMBRUZZI, W. **Educação em Engenharia e Mineração de Dados Educacionais: oportunidades para o tratamento da evasão.** Revista: EaD & Tecnologias Digitais na Educação, Dourados, MS, v.2, n.03, Jan/Nov, 2014.

RODRIGUEZ, A. L. T. **Inteligencia artificial y ética de la responsabilidad. Cuestiones de Filosofía**, v.4 n. 22, p.141-170, 2018. doi: https://doi.org/10.19053/01235095.v4.n22.2018.

SANTOS, E. **Educação online para além da EAD: Um fenômeno da cibercultura**. Actas do X Congresso Internacional Galego-Português de Psicopedagogia. Braga: Universidade do Minho, 2009.

SCLATER, N. **A literature review of the ethical and legal issues. Code of practice for learning analytics**. 2014. Disponível em: http://www.wojde.org/FileUpload/bs295854/File/07rp_54.pdf. Acesso em: 4 de maio de 2020.

SENIOR SISTEMAS S.A. **Workflow - Manual do Usuário / Análise de desempenho / Disponibilização de dados**, 2020. Disponível em: https://documentacao.senior.com.br/workflow/6.2.33/wfe/disp_dados/wfe_dispdados.htm. Acesso em: 05 de maio de 2020.

SILVA, C.A. **O elo mais fraco da segurança da informação: Pessoas representam o maior desafio**. Kindle Edition, 2015.

SILVA, D.; MAMEDIO, P. M. **A relação professor x aluno para o ensino aprendizagem.** Anais do Congresso de Iniciação Científica, Estágio e Docência do Campus Formosa, 2016

SILVEIRA, A., PORTELLA, A. **Tratamento de dados pessoais em meio à pandemia de covid-19: comentários sobre o adiamento do início da vigência da LGPD,** 2020. Disponível em : https://www.migalhas.com.br/depeso/326070/tratamento-de-dados-pessoais-em-meio-a-pandemia-de-covid-19-comentarios-sobre-o-adiamento-do-inicio-da-vigencia-da-lgpd. Acesso em: 06 de maio de 2020.

SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. **Código de Ética do Profissional da Informática.** 2013. Disponível em: https://www.sbc.org.br/institucional-3/codigo-de-etica. Acesso em: 06 de maio de 2020.

SOPRANA, P. **Zoom corre para corrigir falhas após invasões; saiba como se proteger**. Folha de São Paulo, São Paulo, 27 de abril de 2020. Disponível em: https://www1.folha.uol.com.br/mercado/2020/04/zoom-corre-para-corrigir-falhas-apos-invasoes-saiba-como-se-proteger.shtml. Acesso em: 05 de maio de 2020.

TEIXEIRA, S. **Preconceito digital: o que acontece quando a IA favorece a discriminação**. Nova York, 2019. Disponível em:.https://ittrends.com/conteudos/preconceito-digital/. Acesso em: 06 de maio de 2020.

TOKAMIA, M. **Menos da metade dos estudantes aprendem sobre segurança na internet**. Empresa Brasil de comunicação. Agência Brasil. 2019. Disponível em:.https://agenciabrasil.ebc.com.br/educacao/noticia/2019-07/menos-da-metade-dos-estudantes-aprende-sobre-seguranca-na-internet . Acesso em: 4 de maio de 2020.

TRAILHEAD. **Visão geral da segurança dos dados. Salesforce Plataform**. Disponível em: https://trailhead.salesforce.com/pt-BR/content/learn/modules/data_security/data_security_overview. Acesso em: 25 de maio de 2020.

TUGENDHATI, E. **Lições sobre ética.** Petrópolis: Vozes, 1999

UNESCO. **Global Monitoring of School closures caused by COVID-19**, 2020. Disponível em: https://en.unesco.org/covid19/educationresponse. Acesso em: 05 de maio de 2020.

UNIVERSIDADE DE MONTREAL. **Montreal declaration for a responsible development of artificial intelligence**. 2018. Disponível em: https://5dcfa4bd-f73a-4de5-94d8-c010ee777609.filesusr.com/ugd/ebc3a3_5c89e007e0de440097cef36dcd69c7b0.pdf Acesso em: 20 de maio de 2020.

WHATSAPP. **Privacy Policy**. 2020. Disponível em: https://www.whatsapp.com/legal?eea=1#privacy-policy. Acesso em: 06 de maio de 2020.

ZOOM. **Declaração legal e de privacidade**, 2020. Disponível em: https://zoom.us/docs/pt-pt/privacy-and-legal.html. Acesso em: 06 de maio de 2020.