Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Contribuições para conduta ética em três momentos na pesquisa em tecnologia educacional:

Implantação, projeto e avaliação

Barbara Varanda Rangel

Monografia apresentada como requisito parcial
para conclusão do Bacharelado em Ciência da Computação

Orientadora
Prof.a Germana Menezes da Nóbrega

Brasília
2021

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Rangel, Bárbara Varanda
RR196c Contribuições para conduta ética em três momentos na pesquisa em tecnologia educacional: Implantação, projeto e avaliação / Bárbara Varanda Rangel; orientador Germana Menezes da Nóbrega. -- Brasília, 2021.
80 p.

Monografia (Graduação - Ciência da Computação) -- Universidade de Brasília, 2021.

1. Ética . 2. Learning Analytics. 3. Termo de Uso. 4. Política de Privacidade. 5. Termo de Consentimento Livre e Esclarecido. I. Nóbrega, Germana Menezes da, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Contribuições para conduta ética em três momentos na pesquisa em tecnologia educacional:

Implantação, projeto e avaliação

Barbara Varanda Rangel

Monografia apresentada como requisito parcial
para conclusão do Bacharelado em Ciência da Computação

Prof.a Germana Menezes da Nóbrega (Orientadora)
CIC/UnB

Prof.a Edna Dias Canedo
CIC/UnB

Prof.a Fernanda Lima
CIC/UnB

Prof. Marcelo Grandi Mandelli
Coordenador do Bacharelado em Ciência da Computação

Brasília, 20 de outubro de 2021

Dedicatória

Dedico esse trabalho primeiramente a minha mãe Diane, que sempre priorizou minha educação com todo o amor do mundo. Além disso dedico esse trabalho a minha esposa Haisa, que é o meu porto seguro e que me fez acreditar que eu conseguiria. Dedico também aos meus amigos que fizeram esses anos de faculdade me tornarem uma pessoa melhor.

Agradecimentos

Agradeço às professoras que me orientaram nessa jornada, inicialmente à Professora Edna Dias Canedo, por me dar uma chance quando nem eu mesma acreditava em mim, e à Professora Germana Menezes, me guiando para finalizar meu curso com uma contribuição tão relevante, por me incentivar a dar meu melhor, me acalmar nos momentos em paralisei de ansiedade e por não me deixar desistir, nem desistir de mim. Agradeço à Maria Helena da secretaria que sem ela eu com certeza não estaria mais na UnB, sempre me ajudou muito e sempre com um sorriso no rosto. Agradeço aos professores e colegas que me incentivaram e me inspiraram. Agradeço também à minha mãe, minha esposa e meus amigos por estarem sempre do meu lado.

Resumo

A tecnologia está cada dia mais presente na educação. Diversas aplicações de contexto educacional envolvem o processamento de dados pessoais, e é necessário pensar em como esse processamento pode ser feito da maneira mais ética possível, tanto no seu funcionamento interno, livre de discriminação e viés, quanto na maneira que os dados são tratados e transferidos entre sistemas, visando a proteção de dados e a privacidade. Este trabalho visa apoiar desenvolvedores e pesquisadores a entenderem os desafios éticos que estão presentes na construção de sistemas de software que interagem com pessoas, mais especificamente alunos, coletando dados e os processando para fazer análises. Para tal, serão construídos, como exemplo, 5 artefatos éticos para o desenvolvimento, a implantação e avaliação da rede social CICFriend, um nó do software Friendica. Para apoiar o desenvolvimento, foi construída uma matriz de riscos e benefícios éticos e operacionais sob a ótica do ciclo de vida de tratamento de dados. Para a implantação foram fornecidas recomendações, requisitos e melhores práticas para a elaboração do: Termo de Uso, Política de Privacidade e Declaração de Privacidade. E para apoiar a pesquisa e a avaliação, foram fornecidas recomendações sobre consentimento informado e um passo a passo da construção do Termo de Consentimento Livre e Esclarecido.

Palavras-chave: Ética, Learning Analytics (LA), Inteligência Artificial (IA), Termo de Consentimento Livre e Esclarecido (TCLE), Termos de Uso, Política de Privacidade

Abstract

Technology is increasingly present in education. Several educational context applications involve the processing of personal data, and it is necessary to think about how this processing can be done in the most ethical way possible, both in its internal functioning, free from discrimination and bias, and in the way in which the data is treated and transferred between systems for data protection and privacy. This work aims to support developers and researchers to understand the ethical challenges that are present in the construction of software systems that interact with people, more specifically students, collecting data and processing them for analysis. To this end, as an example, 5 ethical artifacts will be built for the development, implementation and evaluation of the CICFriend social network, a node of the Friendica software. To support the development, a matrix of ethical and operational risks and benefits was built from the perspective of the data processing lifecycle. For the implementation, recommendations, requirements and best practices were provided for the elaboration of: Terms of Use, Privacy Policy and Privacy Statement. And to support the research and evaluation, recommendations were provided on informed consent and a step-by-step construction of the Free and Informed Consent Form.

Keywords: Ethics, Learning Analytics (LA), Artificial Intelligence (AI), Free Prior and Informed Consent (TCLE), Terms and conditions of use, Privacy Policy

Sumário

1 Introdução **1**

1.1 Contextualização 1

1.2 Motivação e Justificativa 2

1.3 Objetivos 3

1.3.1 Objetivo Geral 3

1.3.2 Objetivos Específicos 3

1.4 Estrutura do documento 3

2 Revisão de literatura: Ética e Learning Analytics **5**

2.1 Ética e Inteligência Artificial 5

2.2 Inteligência Artificial na Educação 7

2.3 Tradição quanto à avaliação de aplicações educacionais 10

2.4 Pauta mais recente: projeto e utilização 12

3 Fundamentação Teórica para a Proposta **16**

3.1 CICFriend, caso de uso para guiar a elaboração dos artefatos 16

3.2 Lei Geral de Proteção de Dados - LGPD 20

3.3 A Privacidade e o Consentimento informado 24

3.4 Desafios e *framework* ético para guiar projeto em tecnologia educacional . . 26

4 Proposta: Contribuições para tecnologia educacional eticamente consciente à luz da CICFriend **34**

4.1 Quanto a Implantação: Termo de Uso, Política de Privacidade e a Declaração de Privacidade 34

4.2 Quanto ao Projeto e Desenvolvimento: Mapa de benefícios e riscos 38

4.3 Quanto a Avaliação: TCLE 41

5 Conclusão **44**

5.1 Objetivos alcançados 44

5.2 Trabalhos futuros 45

Referências **47**

Apêndice **52**

A Termo de Uso, Política de Privacidade e Declaração de Privacidade CIC-Friend **53**

A.1 Declaração de Privacidade 53

A.2 Termo de Uso 54

A.3 Política de Privacidade 59

B Matriz de Riscos e Benefícios **66**

C Termo de Consentimento Livre e Esclarecido CICFriend **68**

Lista de Figuras

2.1 Diferença entre IAED e *Learning Analytics*. 9
2.2 Esboço conceitual para *framework* ético para a IAED. 10

3.1 Visão da arquitetura atualmente proposta para o ecossistema. 18

4.1 Matriz de riscos e benefícios. 39

Lista de Tabelas

3.1 Recomendações para aprimorar formulários de consentimento baseadas na literatura 26

4.1 Fases do ciclo de vida e respectivas operações de tratamento 40

Capítulo 1

Introdução

1.1 Contextualização

De acordo com especialistas, estamos vivendo hoje a quarta revolução industrial, caracterizada pelas tecnologias emergentes que estão redefinindo os modos de comunicação, de informação, de entretenimento, de trabalho e de aprendizado [1].E no centro dessa revolução está a Inteligência Artificial (IA), sistemas que exibem comportamento inteligente ao analisar seu ambiente e tomar ações - com algum grau de autonomia - para atingir objetivos específicos [2].

A educação e o conhecimento são pilares desse processo de evolução tecnológica [3] e o advento da IA abre um imenso campo de possibilidades para a compreensão dos diversos desafios atrelados ao ensino como: o quão eficaz é um curso, se atende as necessidades dos alunos, quais interações são mais eficazes, como elas podem ser melhoradas, como melhor apoiar professores para alcançar o sucesso individual de estudantes, como apoiar administradores a atingirem suas metas, como identificar alunos em risco de reprovação, como identificar alunos líderes, dentre outros [4].

A Internet é utilizada por aproximadamente 134 milhões de brasileiros cotidianamente [5], que em sua maioria utilizam redes sociais. Diversos artigos elaboram os potenciais benefícios do uso de redes sociais em ambiente acadêmico e como a análise dos dados dessas redes podem trazer informações relevantes ao contexto estudantil [6].

Enquanto o uso de IA na educação tem crescido [7], e as regulações quanto à utilização de dados pessoais tem sido implementadas por todo o mundo, os dilemas quanto ao seu uso ético tem ficado em segundo plano. Porém, como descrito em Lawson et al [8], as implicações éticas sobre questões como direito sobre os dados, vigilância e rotulagem, podem afetar a relação de confiança entre o aluno e a instituição de ensino, assim como prejudicar ao invés de apoiar a aprendizagem do estudante.

A Lei Geral de Proteção de Dados (LGPD) foi aprovada dia 14 de agosto de 2018 e regulamenta as operações de tratamento de dados realizadas em território nacional. Essa lei visa proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural [9].

Diversas aplicações de contexto educacional envolvem o processamento de dados pessoais, e para isso é necessário pensar em como esse processamento pode ser feito da maneira mais ética possível, tanto no seu funcionamento interno, livre de discriminação e preconceito, quanto na maneira que os dados são tratados e transferidos entre sistemas, visando a proteção de dados e a privacidade.

1.2 Motivação e Justificativa

O projeto smartUnB.ECOS [10] estuda e visa implantar, avaliar e manter um ecossistema de e-learning para a Universidade de Brasília, que reúna diversos sistemas e funcionalidades de maneira interoperável. Conforme apontado pela literatura, é necessário pensar nas questões de ética, privacidade e direito de dados dos alunos antes da implementação, seguindo as diretrizes de *privacy by design* e *ethically aligned design*.

Este trabalho visa apoiar desenvolvedores e pesquisadores a entenderem os desafios éticos que estão presentes na construção de sistemas de software que interagem com pessoas, mais especificamente alunos, coletando dados e os processando para fazer análises. Para tal, serão construídos como exemplo os artefatos éticos necessários para o desenvolvimento, a implantação e avaliação da rede social CICFriend, um nó do software Friendica, uma rede social de código aberto e descentralizado que está sendo implantado como ferramenta interação para alunos dos cursos de Computação na UnB.

Parte-se do pressuposto que apresentar diretrizes e boas práticas de desenvolvimento ético colabora para a criação de uma cultura de proteção de dados e de pensamento ético. Mostrar o passo a passo da construção de um Termo de Uso e uma Política de Privacidade, requisito para implantação de um sistema, que sejam éticos, claros e complacentes à LGPD, fornece à comunidade um ponto de partida para aumentar a transparência na relação entre usuário e controlador de dados. E explicar a necessidade de elaborar um Termo de Consentimento Livre e Esclarecido, requisito para pesquisa e avaliação, que apoie o aluno participante a compreender melhor como seus dados serão usados e a sua expectativa de privacidade, demonstra ao pesquisador que o consentimento informado não é apenas uma prática moral mas também aumenta a confiança entre pesquisador e participante, trazendo benefícios a ambos.

1.3 Objetivos

1.3.1 Objetivo Geral

O objetivo deste trabalho é propor um conjunto de artefatos para facilitar a conduta ética em pesquisas em tecnologias educacionais, juntamente com um elenco de recomendações que permitam sua reutilização.

1.3.2 Objetivos Específicos

- Propor uma Declaração de Privacidade que seja de rápida leitura, fácil compreensão, que englobe os principais pontos abordados no Termo de Uso e na Política de Privacidade, com o objetivo de ser apresentada ao usuário antes do consentimento ao processamento de dados pessoais para aumentar a probabilidade da leitura pelo usuário, aumentando assim o consentimento informado.

- Propor um Termo de Uso e uma Política de Privacidade que seja de fácil compreensão, transparente sobre o processamento de dados ocorrido e aderente à Lei Geral de Proteção de Dados.

- Propor um Mapa de Benefícios e Riscos que explicite os riscos de cada momento do tratamento de dados pessoais, colaborando assim para uma conduta ética no desenvolvimento da solução e no gerenciamento de dados estudantis e como apoio para a elaboração dos Termos de Uso e de Consentimento Livre e Esclarecido.

- Propor um Termo de Consentimento Livre e Esclarecido que seja de linguagem simples, descritivo, e que elucide todo possível risco e benefício atrelado à participação do aluno na pesquisa.

1.4 Estrutura do documento

Este trabalho está organizado em cinco capítulos, incluindo esta introdução.

No Capítulo 2 são apresentados os principais conceitos abordados neste trabalho, iniciando com a perspectiva da ética na IA, apresentação do campo da Inteligência Artificial na Educação (IAED) e abordando como é realizada a pesquisa na área. Em seguida é apresentada uma revisão de literatura em linha de tempo com artigos relacionados à ética em *Learning Analytics* e na IAED, utilizados como plano de fundo para a elaboração das contribuições que seguem.

No Capítulo 3 é realizada a apresentação do referencial teórico utilizado como base no desenvolvimento deste trabalho e na criação dos artefatos propostos. Primeiramente

apresenta-se o caso de uso que será base para elaboração dos artefatos, a rede social CICFriend, e suas principais características, especialmente que tratam de privacidade. Em seguida é abordada a Lei Geral de Proteção de dados, seus fundamentos e princípios, os direitos dos usuários e as hipóteses para o tratamento de dados pessoais. A principal dessas hipóteses é o consentimento, que é então abordado em nova seção sobre privacidade e os desafios do consentimento informado, especificando como o desenvolvimento do Big Data e da IA tem impactado esse campo. O capítulo é encerrado abordando os desafios éticos encontrados na revisão de literatura realizada, e os princípios propostos para um framework ético para *Learning Analytics*.

No Capitulo 4 é apresentada então a proposta, em 3 seções divididas de acordo com os diferentes momentos de aplicação dos artefatos. A primeira seção é a implantação, os artefatos são o Termo de Uso e a Política de Privacidade, e suas respectivas construções, desde a conceitualização até as melhores práticas, são descritas. Foi proposto também um novo artefato, a Declaração de Privacidade, como tentativa de aumentar o consentimento informado. A segunda seção é de projeto e desenvolvimento, em que é proposta a construção de um mapa de benefícios e riscos relacionados às etapas do ciclo de vida do tratamento de dados, adicionando uma visão das questões éticas centrais relevantes para cada momento e perguntas orientadoras para guiar reflexão sobre possíveis implicações éticas do projeto. A terceira e última seção se refere à avaliação, é apresentado o Termo de Consentimento Livre e Estabelecido, requisito para realização de pesquisa sobre humanos, são citadas as resoluções normativas que guiam as pesquisas, e são listadas recomendações para a elaboração do documento.

O Capítulo 5 encerra o trabalho apresentando os objetivos alcançados e os projetos futuros.

Nos apêndices, são apresentados os artefatos:

Apêndice A - A Declaração de Privacidade, o Termo de Uso e a Política de Privacidade.

Apêndice B - Matriz de riscos e benefícios.

Apêndice C - Termo de Consentimento Livre e Esclarecido.

Capítulo 2

Revisão de literatura: Ética e Learning Analytics

Neste capítulo serão apresentados os principais conceitos relevantes a este trabalho e o referencial teórico necessário para entender a sua contextualização. Serão abordados: o conceito de Inteligência Artificial e sua relação com a ética, o uso da Inteligência Artificial na Educação, a tradição quanto a avaliação ética de pesquisas e então a revisão de literatura em Ética e Análise de Aprendizado.

2.1 Ética e Inteligência Artificial

O Grupo de Especialistas de Alto Nível em IA (AI HLEG) [11], estabelecido pela Comissão da EU, define sistemas de IA como:

> "Os sistemas de inteligência artificial (IA) são sistemas de software (e possivelmente também hardware) projetados por humanos que, atendendo a um objetivo complexo, atuam na dimensão física ou digital percebendo seu ambiente por meio da aquisição de dados, interpretando os dados estruturados ou não estruturados coletados, raciocinando sobre o conhecimento ou processando as informações derivadas desses dados, e decidindo a melhor ação a ser tomada para atingir o objetivo dado. Os sistemas de IA podem usar regras simbólicas ou aprender um modelo numérico e também podem adaptar seu comportamento, analisando como o ambiente é afetado por suas ações anteriores".

Os dados são o combustível para o treinamento de sistemas de IA e a cada segundo, milhões de dados de todos os tipos de transações e acessos a sistemas digitais são gerados e armazenados. Ray Kurzweil em seu livro "Como criar uma mente" fala sobre as vantagens do desenvolvimento tecnológico [12].

> "Por meio de tecnologias, podemos enfrentar os grandes desafios da humanidade, como manter um meio ambiente saudável, fornecer recursos para uma população

> crescente (incluindo energia, alimentos e água), superar doenças, estender amplamente a longevidade humana e eliminar a pobreza. É apenas estendendo-nos com tecnologia inteligente que podemos lidar com a escala de complexidade necessária."

A IA pode solucionar muitos problemas latentes da sociedade atual, porém também existem grandes riscos atrelados a seu mal uso. O modelo aprendido por um sistema de aprendizado de máquina é tão bom quanto os dados com os quais é treinado. Quando esses dados contêm vieses ou valores errôneos, ou quando não são obtidos de maneira adequada que garantem a privacidade e são baseadas no consentimento, o algoritmo pode levar a conclusões preconceituosas ou erradas.

Vale ressaltar também que as coletas de dados são realizadas com um objetivo, com base em um conjunto de expectativas, o que significa que contêm a configuração estatística, as preferências ou o viés de quem os coletou. Portanto, é importante garantir a transparência dos processos e abordagens de tomada de decisão, bem como a governança adequada dos dados.

O desenvolvimento da IA e sua junção com o Big Data (processamento de grandes volumes de dados) podem gerar muitas novas oportunidades mas também sérias ameaças à sociedade. A desvalorização do trabalho, o aumento da concentração de riquezas levando a monopólios de mercado, a possibilidade de estar sujeito a: vigilância generalizada, ao controle de acesso a informações e oportunidades, a manipulação através criação de perfis para direcionar propagandas ou mudar opiniões, são somente alguns dos riscos provenientes do uso da IA que foram citados por Sartor [13] em artigo publicado a pedido do Painel para o Futuro da Ciência e Tecnologia, do Serviço de Pesquisas do Parlamento Europeu.

Soluções de IA podem ser criadas para inferir informações de indivíduos ou grupos, ou seja, expandir os dados disponíveis de maneira a descrever ou antecipar suas características e propensões, o que pode ser utilizada de maneira maléfica ou benéfica. Por exemplo, no caso em que a característica inferida de um indivíduo é sua maior suscetibilidade ao câncer, a indicação do sistema pode servir de base para oferecer melhores terapias e exames preventivos ou para o aumento do valor do seguro de saúde [13].

A informação inferida pode também consistir na propensão a reagir de certa forma a determinados *inputs*. No âmbito educacional por exemplo, pode consistir na propensão de responder a um certo tipo de publicação ou a uma certa atividade proposta como um certo comportamento de engajamento com material e com os outros alunos, ou pode consistir na propensão de responder a um certo tipo de mensagem com uma mudança de humor ou preferência por curso. Por exemplo, no caso de um aluno em risco de reprovação, a propensão do aluno reagir estudando mais a uma mensagem de apoio propondo suporte ou a uma mensagem ameaçadora que realça a propensão de reprovação.

A Comissão Europeia em uma publicação de fevereiro de 2020 [14] afirmou que a IA:

> "mudará as nossas vidas ao melhorar os cuidados de saúde (por exemplo, tornando o diagnóstico mais preciso, permitindo uma melhor prevenção de doenças), aumentando a eficiência da agricultura, contribuindo para a mitigação e adaptação às alterações climáticas, melhorando a eficiência dos sistemas de produção através da manutenção preditiva, aumentando a segurança dos europeus , e de muitas outras maneiras que só podemos começar a imaginar."

A IA já está sendo utilizada nos mais diversos campos de conhecimento e são diversos os exemplos do seu uso, como a tradução instantânea de uma transmissão de vídeo, verificação de fraude de identidade nos aeroportos através do reconhecimento facial, reconhecimento da ação de um arquivo malicioso, apoio para que médicos realizem diagnósticos mais precisos, dentre outros.

Os impactos do seu mal uso também já foram sentidos nos últimos anos, como por exemplo no caso da Cambridge Analytica de 2018. A Cambridge Analytica era uma empresa de consultoria política britânica, que coletou sem permissão dados de 87 milhões de usuários da rede social Facebook, além de outras fontes públicas e privadas [15], e os utilizou para micro-direcionar mensagens mais prováveis de influenciar o comportamento individual de eleitores. Para realizar esse direcionamento foi desenvolvido um modelo que traduzia os dados pessoais em um perfil de personalidade usado para prever e, em seguida, mudar o comportamento [16].

Os dados foram coletados através de um aplicativo chamado "This is your digital life", em que aproximadamente 300 mil indivíduos [17] foram pagos para preencher um questionário dito que seria para uso acadêmico. Para preenche-lo os usuários tinham que consentir a fornecer acesso a todos os seus dados do Facebook, porém, a plataforma do Facebook permitiu acesso não somente aos dados dos usuários, mas também de seus amigos da rede social, e com isso conseguiu traçar o perfil de milhões de eleitores americanos, podendo ter impactado no resultado das eleições americanas e de outros países em que a empresa prestou consultoria, incluindo o Brasil [18].

São diversos os potenciais benefícios e riscos, e é necessário que esse progresso seja controlado através de regulações, normas e *frameworks* que possibilitem que essa tecnologia seja utilizada de maneira ética e legal.

2.2 Inteligência Artificial na Educação

A Inteligência Artificial na Educação (IAED) [1] trata sobre as diversas maneiras em que sistemas de IA podem ser utilizados para apoiar a aprendizagem formal e informal, e

[1] Maiores eventos da comunidade: `https://aied2021.science.uu.nl/` e `https://its2021.iis-international.org/`

engloba duas vertentes complementares: o desenvolvimento de ferramentas baseadas em IA para apoiar a aprendizagem e a utilização dessas ferramentas para ajudar a compreender o processo de aprendizagem. Por exemplo, ao modelar como os alunos resolvem um problema aritmético, caso sejam identificados usos de conceitos errôneos por parte dos alunos anteriormente desconhecidos dos educadores, pesquisadores e professores podem começar a entender mais sobre o próprio processo de aprendizagem que pode então ser aplicado a práticas de sala de aula [19].

Assim como grande parte das áreas da IA, a IAED frequentemente utiliza modelos computacionais para representar diferentes aspectos chave envolvidos no resultado. Sistemas de tutoria inteligente, por exemplo, usam 4 modelos, 3 principais e um recomendado para monitoração e controle, que interagem de maneiras complexas e são combinados para adaptar uma sequência de atividades de aprendizado para cada aluno:

1. Modelo Pedagógico

   Conhecimento sobre abordagens eficazes de ensino e aprendizagem que foram extraídas de especialistas em ensino;

2. Modelo de Domínio

   Conhecimento sobre o assunto que o sistema visa ajudar os alunos a aprender;

3. Modelo do Aluno

   Conhecimento sobre os alunos, tanto de todos os alunos que usaram o sistema até agora quanto do aluno individual que o está utilizando.

4. Modelo OpenLearner

   Dar visibilidade à alunos e professores do caminho percorrido pelo aluno e as tomada de decisão do sistema.

Uma área em crescimento dentro de IAED é a *Learning Analytics* (LA - Analíticas de Aprendizagem), e uma das suas primeiras definições é de Siemens 2011:

> "*Learning Analytics* se trata da medida, coleta, analise e relatório de dados sobre alunos e seus contextos, no propósito de entender e otimizar o aprendizado e o ambiente onde ele ocorre."

As distinções entre Sistemas de *Learning Analytics* (LA) e sistemas de IAED estão cada vez menores, mas a principal diferença é que sistemas de LA usualmente utilizam as análises e dados coletados para apoiar na intervenção humana, e sistemas de IAED os utilizam para iniciar alguma intervenção automatizada. A Figura 2.1 representa graficamente essa diferença.

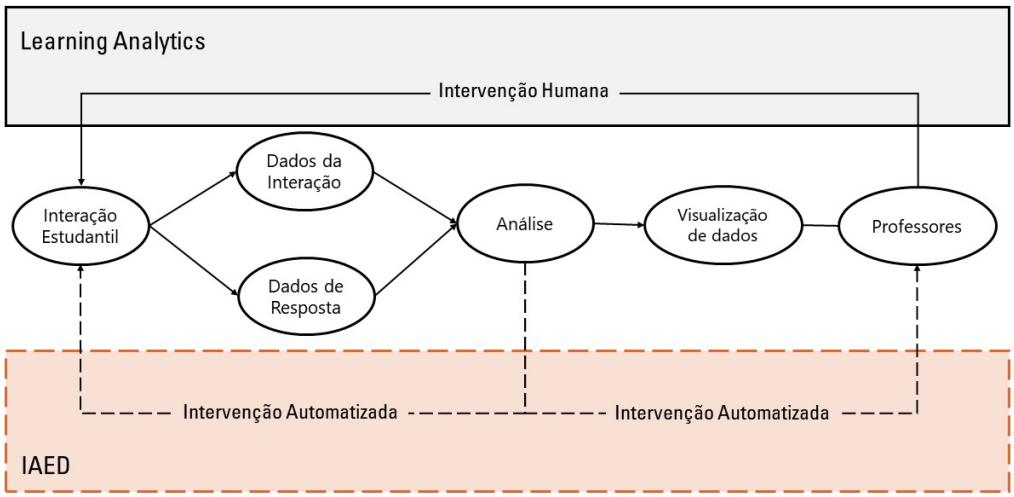

Figura 2.1: Diferença entre IAED e *Learning Analytics* (Fonte: [19]).

Uma revisão de literatura sobre os principais *frameworks* e os desafios éticos com um maior foco em *Learning Analytics* será realizada no próximo tópico, porém exitem desafios éticos específicos da IAED que são de grande relevância, visto que é o futuro idealizado do projeto SmartUnB.ECOS. Holmes [19] cita alguns desses desafios e dilemas em termos dos 3 modelos principais inseridos acima:

- Pedagógico

  Impacto da IAED nas relações pedagógicas, tipos de informações usadas para justificar uma intervenção automatizada e as mudanças comportamentais esperadas.

- Domínio

  Impacto da adaptação do conteúdo de uma disciplina específica pela IAED e sua influência na experiência do aluno, na sua compreensão desse conteúdo e na segregação do nível de aprendizado dos alunos.

- Aluno

  Impacto sobre a vigilância estudantil, tensão entre sistemas paternalistas e a autonomia do aluno, natureza transitória de objetivos, emoções e interesses dos alunos.

Holmes et al [20], se aprofunda no estudo da ética da IA na educação, e propõe um esboço conceitual para um *framework* compreensivo em IAED, representado pela

Figura 2.1. Este esboço representa as 6 áreas da ética que devem ser consideradas ao pensar em ética da IAED. A interrogação central representa as chamadas "incógnitas desconhecidas", questões éticas levantadas pela AIED que ainda precisam ser identificadas (ou seja, questões na interseção central entre dados, computação e educação, e a interação específica entre o uso de sistemas de IA e a cognição humana no nível individual).

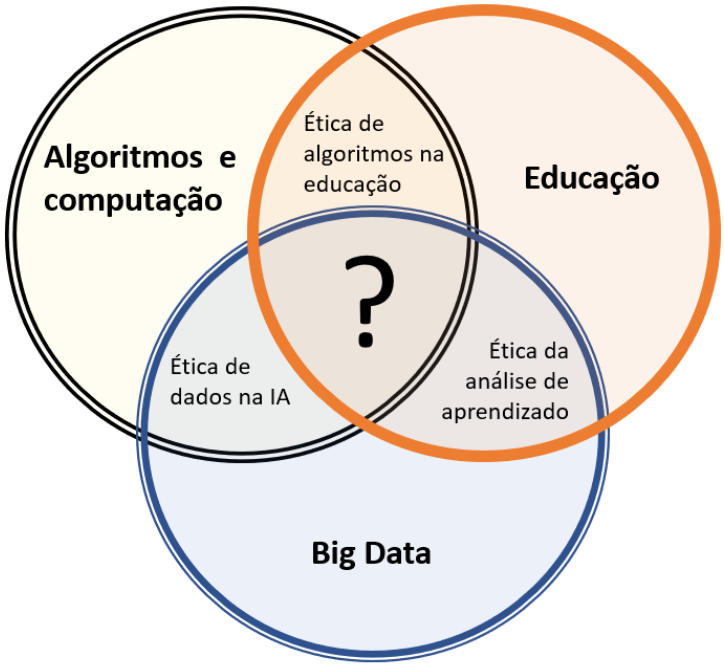

Figura 2.2: Esboço conceitual para *framework* ético para a IAED (Fonte: [20]).

Ao fazer esse esboço Holmes chama a atenção para a necessidade de se ter uma visão ampla sobre a ética na IAED, da relevância desse campo de estudo, e como essas contribuições podem apoiar debates mais amplos sobre as maneiras pelas quais a AI pode impactar a cognição humana e a tomada de decisões.

2.3 Tradição quanto à avaliação de aplicações educacionais

Para que seja realizada a avaliação de uma aplicação educacional é necessário que seja realizada uma pesquisa com os usuários, além de uma análise da utilização da aplicação, que demanda coletas de dados pessoais. Para a realização desse tipo de pesquisa, especialmente no âmbito da universidade, é necessária a aprovação de um Comitê de Ética.

No Brasil a primeira resolução que trata de pesquisas sobre humanos é do Conselho Nacional de Saúde (CNS) 196/96, fundamenta-se nos principais documentos internacionais que emanaram declarações e diretrizes sobre o assunto, visa assegurar os direitos e deveres que dizem respeito à comunidade científica, aos sujeitos da pesquisa e ao Estado e estabelece os Comitês de Ética em Pesquisa (CEP) [21].

Em 2012, surge a resolução do CNS 466/12, mantendo os mesmos princípios éticos da anterior porém aumentando definições e estabelecendo processos com relação ao consentimento livre e esclarecido. Cita algumas especificidades da área das ciências Humanas e Sociais, porém não prevê regulamentação diferenciada [22].

Em 2016, uma nova resolução, a CNS 510/16 [23] expande esse reconhecimento, criando um conjunto mais adequado de princípios e normas para avaliação ética de pesquisas cientificas de abordagem mais qualitativa, não condicionadas a conceitos de neutralidade e cientificidade tão rígidos [24].

Então para a realização de uma pesquisa que envolva seres humanos é previsto por lei que o projeto seja submetido a um Comitê de Ética. Para projetos de pesquisa em Informática na Educação, que inclui projetos de pesquisa de tecnologia educacional, existe uma importante referência sobre o assunto no livro Metodologia de Pesquisa Científica em Informática na Educação: Concepção de Pesquisa, o capítulo 7, Submissão de projeto de pesquisa ao Comitê de Ética: da Plataforma Brasil ao Parecer Consubstanciado [25].

Fronza neste capítulo apresenta considerações e o passo a passo de todo o processo para a submissão de um projeto de pesquisa, iniciado pelo cadastro na Plataforma Brasil e que segue com a avaliação de um Comitê de Ética em Pesquisa (CEP) até o parecer consubstanciado. Com isso fornece aos pesquisadores conhecimento sobre: os principais passos para submeter o projeto; a importância da indicação clara dos possíveis riscos decorrentes da pesquisa e benefícios previstos; a necessidade de se explicitar o desenho metodológico do estudo e suas implicações éticas; e as informações que não podem faltar nos documentos de apresentação obrigatória à submissão do projeto ao CEP.

Essa importante referência, juntamente com as resoluções do Conselho Nacional de Saúde (CNS), os modelos disponíveis da Comissão de Ética em Pesquisa em Ciências Humanas e Sociais (CEP CHS) da UnB, e as melhores práticas quanto ao consentimento informado disponíveis na literatura que será abordado no próximo capítulo embasam a criação do Termo de Consentimento Livre e Esclarecido exemplo para a pesquisa sobre a usabilidade e potenciais benefícios da utilização da aplicação CiCFriend no contexto educacional do Departamento de Ciência da Computação da Universidade de Brasília.

2.4 Pauta mais recente: projeto e utilização

Slade e Prinsloo [26], em artigo de 2013, referenciam as pesquisas anteriores em ética em *Learning Analytics* e outros campos relacionados à tecnologias educacionais, adicionam uma visão geral integrada das principais questões éticas envolvendo *Learning Analytics* (LA) sob uma perspectiva sócio-crítica. Propõem então um conjunto de 6 princípios éticos para guiar o uso de LA que tratam sobre seu uso de forma transparente e moral, da sua importância para maior entendimento do processo de aprendizagem, da importância da participação ativa do aluno e de considerar que os alunos estão em constante evolução. Conclui propondo uma série de considerações para abordar as principais questões que surgem ao implementar uma solução de LA.

Pardo et al. [27], em artigo publicado em 2014, fazem uma análise de como a privacidade e as questões éticas se aplicam ao contexto de *Learning Analytics* e propõem diretrizes para cumprir os princípios de privacidade mais comuns emergentes em várias iniciativas legislativas. Para essa analise é realizada uma comparação de como áreas de estudo como a medicina lidaram com questões de privacidade ao coletar informações privadas. Quatro princípios foram identificados para categorizar as diversas questões derivadas da privacidade: transparência, controle do aluno sobre os dados, segurança e responsabilidade e avaliação contínua. Ao discutir os vários aspectos dentro de cada categoria, os autores colaboram para que instituições construam mecanismos para avaliar as iniciativas em LA e obter conformidade com as leis e regulamentos atuais, bem como com requisitos derivados socialmente.

Lawson et al. [8], em artigo de 2016, apresentam um estudo de caso do sistema EASI (Early Alert Student Indicators - Indicadores de alerta precoce do aluno) de LA utilizado em uma universidade australiana. Esse sistema foi desenvolvido com o objetivo de aumentar a retenção e o sucesso estudantil, porém as implicações éticas não foram consideradas, principalmente com relação ao uso indevido de dados estudantis, coletados de forma consensual na matrícula, porém analisados além do escopo do consentimento original e o uso dessa análise de uma maneira não pretendida pelos designers do sistema, interpretando dados individualizados de alunos para rotulá-los com base em sua estimativa de sucesso. Os dilemas éticos são então explorados mais a fundo, com base no artigo de Slade et al. [26], e as considerações e evoluções feitas pela universidade para tratar cada um desses dilemas é citada. Os autores finalizam lembrando dos potenciais benefícios dos sistemas de LA e da importância de considerar o impacto nos direitos éticos do aluno na implementação desse tipo de sistema.

Prisnloo e Slade [28], em artigo de 2017, abordam o estado da arte da pesquisa de campo em ética em LA, fazendo uma revisão das suas publicações até o momento, destacando os principais estudos publicados sobre as questões éticas em torno de LA, utilizando

como plano de fundo os avanços tecnológicos e as preocupações crescentes em torno da vigilância generalizada e do papel e consequências não intencionais dos algoritmos. Os autores concluem citando como cada um dos *frameworks*, códigos de práticas e mapeamentos conceituais das implicações éticas em LA discutidos adiciona ao entendimento de como podemos caminhar para uma utilização de sistemas de LA éticos.

Slade e Tait [29], publicaram em 2019 um conjunto de diretrizes globais para melhores práticas éticas em *Learning Analytics*, à pedido do Conselho Internacional para Educação Aberta e a Distância (International Council for Open and Distance Education - ICDE)[2]. Este relatório tem como objetivo identificar uma série de questões essenciais, agrupadas em 9 categorias, que propõe serem de relevância global para o uso e desenvolvimento de *Learning Analytics* de maneiras éticas e com isso, então, abrir o espaço de discussão e auxiliar no possível desenvolvimento de diretrizes nacionais para o uso de LA.

Kitto e Knight [30], em artigo de 2019, focam no lado prático de como apoiar desenvolvedores na construção de soluções de LA para adoção institucional. Através de três exemplos, os autores demonstram como alguns dos *frameworks* fornecem pouca orientação sobre alguns dos dilemas práticos enfrentados por desenvolvedores, principalmente em relação as iniciativas regulatórias versus as diretrizes éticas. Em seguida usam de casos de uso extremos para destacar onde os *frameworks* éticos existentes não guiam os construtores, propondo então a construção de um banco de dados aberto de casos extremos relativos ao uso de LA na educação para que os cenários que causam dificuldades possam ser relatados e os protocolos emergentes para lidar com eles listados.

Ferguson [31], em artigo de 2019, responde ao artigo de Selwyn [32] - o que há de errado com *Learning Analytics*? também de 2019, oferecendo uma perspectiva ética relacionando as questões levantadas por ele a uma vertente de trabalho de longa data no campo que lida com a ética de LA, enquadrando essas questões nas seis grandes áreas de desafios éticos identificadas anteriormente. Adiciona como as considerações de Selwyn aumentam o entendimento de cada um desses desafios, que são então expandidos para acomodar melhor os questionamentos levantados.

Holmes et al [33] lançam, também em 2019, uma chamada para um *workshop* na conferência internacional de inteligência artificial na educação, para compartilhar *insights*, identificar questões éticas chaves, mapear como enfrentar os vários desafios e informar as melhores práticas de uma implementação ética de soluções em AIED. Na chamada são colocadas algumas questões chaves e a comunidade é convidada a colaborar para a construção de uma fundação ética sólida para futuras pesquisas em IAED.

Em apoio ao dialogo sobre IA da G20, Vincent-Lancrin et al [34], lançou artigo sobre os desafios e as promessas do uso confiável da IA na educação. Nele são apresentados alguns

[2] `https://www.icde.org/`

usos promissores da IA em salas de aula e no sistema educacional, e algumas maneiras possíveis de fortalecer a aquisição de habilidades mais complexas, como criatividade, pensamento crítico, comunicação ou colaboração. Em seguida, analisa as oportunidades e desafios que a IA pode criar para educadores e formuladores de políticas,

Sobre a questão do consentimento informado, Beardsley [35], publicou artigo sobre uma pesquisa empírica realizada com estudantes do primeiro ano de faculdade para entender se aumentar a ciência dos riscos envolvendo compartilhamento de dados estudantis diminuiria a taxa de participação em estudos. Por se tratar de um cenário específico de uma turma o autor não generalizou seus achados, porém identificou que o aumento da ciência dos riscos não diminuiu a taxa de participação e que estudantes que foram preparados anteriormente citaram mais confiança como fator que influenciou a decisão a compartilhar os dados.

Uma revisão sistemática de literatura sobre ética em LA foi publicada em 2021, mapeando as pesquisas empíricas de ética em LA no ensino superior já realizadas [36]. O estudo responde a 3 questões: como as pesquisas foram realizadas, quais são as principais questões éticas endereçadas e quais são as lacunas de conhecimento identificadas. Os resultados da revisão mostram que a maioria dos estudos são realizados através de entrevistas ou questionários, as 3 principais áreas da ética abordadas foram transparência, privacidade e consentimento informado e que existem diversas lacunas na pesquisa, como uma falta de pesquisa em como instituições devem intervir após a identificação de necessidade de suporte para alunos, mais pesquisas com casos reais para que seja possível identificar contextos similares e mais estudos sobre as perspectivas das diferentes partes interessadas.

Com o objetivo de entender melhor o que a comunidade de pesquisadores em AIED pensa sobre ética, Holmes et al [20], publicou artigo em que convida pesquisadores a responder perguntas sobre ética e a aplicação de IA em contextos educacionais e resume as contribuições dos 17 entrevistados, discutindo então as questões complexas que foram levantadas. Os resultados incluem o reconhecimento de que a maioria dos pesquisadores em AIED não estão treinados para lidar com as questões éticas emergentes e que se faz necessário uma abordagem mais objetiva para ética na AIED, tanto para garantir que as ferramentas e abordagens desenvolvidas pela comunidade sejam éticas por design, quanto para dar mais visibilidade ao trabalho realizado podendo apoiar os outros subcampos de IA e as políticas relacionadas.


2013
Slade e Prinsloo
Apresenta uma visão integrada das principais questões éticas em LA e propõe um conjunto de 6 princípios para guiar seu uso.
2014
Pardo e Siemens
Levanta questões éticas sobre privacidade no contexto de LA, identificando 4 princípios para categorizá-las.
2016
Ferguson et al.
Apresentam algumas das ferramentas práticas desenvolvidas para a implantação de um sistema de LA, e depois apresentam uma tabela com 21 desafios de LA com dimensões éticas
2016
Lawson et al.
Estudo de caso sobre sistema de LA implementado em universidade australiana e os dilemas éticos que seu uso gerou.
2017
Prinsloo e Slade
Revisão de principais publicações sobre ética em LA e como elas adicionam à caminhada para uma LA ética
2019
Slade et al
Conjunto de diretrizes globais para melhores práticas éticas em Learning Analytics.
2019
Kitto e Knight
Utiliza casos de uso extremos para identificar como os frameworks fornecem pouca orientação a questões práticas propondo a construção de um banco de dados desses casos para criar então protocolos para lidar com eles.
2019
Ferguson
Responde ao artigo de Selwyn enquadrando suas questões nas áreas de desafios éticos identificados.
2019
Holmes et al
Chamada para workshop para identificar questões éticas e mapear como enfrentar desafios éticos e informar melhores práticas éticas em AIED.
2020
Lancrin
Apresenta usos promissores da IA na educação e analisa as oportunidades e desafios para educadores e formuladores de políticas.
2020
Beardsley
Pesquisa empírica sobre consentimento informado para verificar se aumentar a ciência dos riscos no compartilhamento de dados afetaria a taxa de participação.
2021
Pargman
Revisão sistemática de literatura que mapeia pesquisas empíricas em LA e identifica lacunas de conhecimento.
2021
Holmes
Apresentam resultados de questionário aplicado à pesquisadores em AIED sobre ética e a aplicação de AI em contextos educacionais

Capítulo 3

Fundamentação Teórica para a Proposta

3.1 CICFriend, caso de uso para guiar a elaboração dos artefatos

Uma rede social é uma estrutura básica da sociedade, uma representação de pessoas (nós) e seus relacionamentos interpessoais (linhas conectoras). O conceito de rede social antecede em quase um século às aplicações que hoje se fazem sinônimo desse termo, e surgiu dos campos da psicologia, antropologia e sociologia, em que teorias de análise de redes sociais, ou seja, das conexões entre as pessoas, apoiavam pesquisadores e estudiosos a entender melhor o funcionamento de dinâmicas de grupo, seja uma dinâmica familiar, de trabalho ou de comunidade [37].

Essa representação da sociedade em rede valoriza conexões e interações horizontais não hierárquicas, e possibilita uma nova forma de agir e pensar, transformando assim os valores envolvidos no contexto social. As plataformas online de redes sociais trouxeram essa visão de sociedade em rede para o cotidiano, ampliando as possibilidades de interação entre as pessoas e provocando uma disruptura em relação à estrutura social convencional [38].

Os potenciais benefícios do uso de uma rede social online no contexto acadêmico foram abordados em revisão de literatura realizada no trabalho que deu início ao projeto CIC-Friend [39] e subsequente artigo [38]. Dentre eles podemos citar: abertura de comunicação entre habitantes do campus considerando as varias esferas de serviços (pedagógico, administrativo, de suporte, entre outros); o aumento da interação e aprendizagem entre pares, entre campi e entre cursos; o uso de recursos de gamificação para aumentar engajamento e mitigar riscos de comportamentos antissociais como o bullying de maneira não punitiva,

através do reforço positivo de atitudes desejáveis, ou seja, recompensa por se comportar bem; dentre outros.

Atualmente, as maiores redes sociais online são baseadas em uma arquitetura centralizada (Facebook, Twitter, LinkedIn, etc) em que o provedor atua como autoridade central e tem controle sobre as informações de usuários, coletando grandes quantidades de dados privados e possivelmente sensíveis de usuários, suas interações, seus comportamentos e estilos de vida. Os usuários dessas redes são obrigados a compartilhar as informações direcionadas aos seus amigos através do provedor de serviço, aumentando o risco de censura, vigilância e revelação de informações, e a profusão dessas diferentes redes centralizadas, cada uma com seu propósito, aumenta esse risco, pois induz usuários a replicarem seus dados em diferentes plataformas e contextos [40].

Para mitigar as questões de privacidade citadas anteriormente e fornecer controle sobre seus dados aos usuários, pesquisadores propuseram descentralizar as funcionalidades das redes sociais, implementando-as de maneira distribuída, e assim surgiram as Redes Sociais Online Descentralizadas (RSOD), tipicamente baseada em uma arquitetura P2P (*peer-to-peer*, ponto-a-ponto, ou de comunicação direta entre usuários) que não tem autoridade central, e são baseadas em um conjuntos de pares que armazenam os conteúdos e executam as tarefas necessárias para fornecer um serviço contínuo.

O Friendica foi escolhido como a rede social online descentralizada e principal forma de comunicação ponto a ponto do projeto SmartUnB.ECOS [10] por ser um software de código aberto altamente personalizável via *addons*, com instalação facilitada, extensas configurações de privacidade, capaz de se federar a outras plataformas de redes sociais tanto descentralizadas quanto centralizadas e que prioriza o controle dos usuários aos próprios dados.

O projeto smartUnB.ECOS [10] estuda e visa implantar, avaliar e manter um ecossistema de e-learning para a Universidade de Brasília, que reúna diversos sistemas e funcionalidades de maneira interoperável. O ecossistema proposto pelo projeto será, de acordo com a Figura 3.1 , inicialmente composto por: um servidor Friendica, um provedor de serviços LTI (especificação para interoperabilidade de tecnologias educacionais), que permitirá que colaborações locais sejam viabilizadas para consumidores LMS (sistemas de gerenciamento de aprendizagem como o Moodle), um sistema de Learning Analytics com armezanamento LRS (armazenamento de registros de aprendizagem que facilita a analise da experiencia do aluno).

A utilização de um sistema de coleta de dados sobre a experiência do aluno juntamente com um sistema de Learning Analytics para prover *insights* sobre a aprendizagem dentro do projeto SmartUnB.ECOS é o principal motivador para o foco deste trabalho em ética e Learning Analytics. O caso de uso do software Friendica na instância denominada

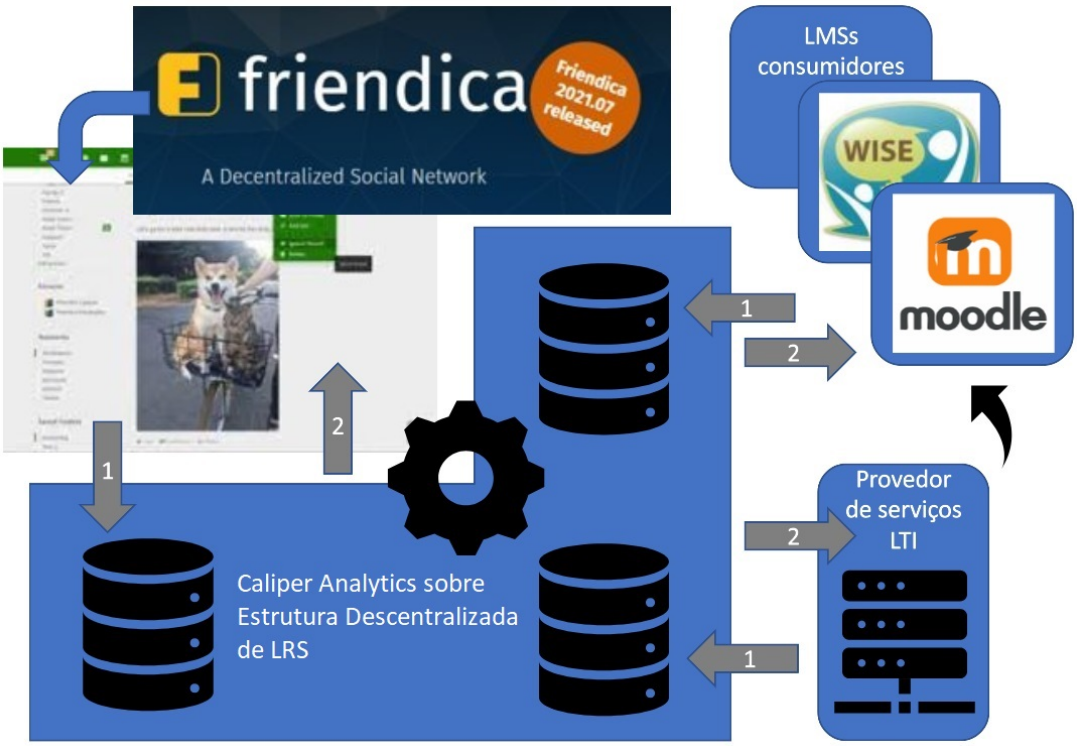

Figura 3.1: Visão da arquitetura atualmente proposta para o ecossistema.

CICFriend é fornecido como exemplo para a construção de subsequentes artefatos para todo o ecossistema.

Principais características [40]:

- Arquitetura P2P não estruturada semi descentralizada - usuários podem ter dispositivos atuando como super *peers* provendo diferentes tipos de serviços; usuários podem decidir fazer parte da rede federada, atuando como servidores Friendica; os conteúdos dos usuários são armazenado em um subconjunto de *peers* desta rede de escolha do usuário; dados não são nativamente encriptados ou replicados, cabendo ao usuário escolher *peers* de confiança.

- Modelo de Privacidade - cada usuário tem um perfil público padrão que pode ser acessado por todos os usuários; o usuário podem restringir o acesso ao seu perfil com base em amigos, protocolos, endereços de e-mail e localização DNS; o usuário pode organizar seus contatos em grupos que podem ser usados para restringir conteúdo; o usuário pode criar grupos privados em que somente ele, o criador do grupo, sabe da existência e dos usuários que o pertencem; o usuário pode configurar perfis distintos para diferentes audiências (ex. perfil pessoal e perfil de trabalho, separando-os por grupos); o usuário pode selecionar múltiplos grupos e amigos específicos que estão

autorizados/não autorizados a acessar conteúdos; o usuário pode ter relações de via única (seguidor).

- Inicialização de Política de Privacidade - usuários são identificados de forma única através do OpenId, protocolo de autenticação de padrão aberto e descentralizado; cada conteúdo publicado pelo usuário é controlado por 4 listas de acesso que especificam os indivíduos e grupos autorizados/ não autorizados a acessar o conteúdo; cada usuário é associado a um nome de usuário e senha utilizados para logar no sistema; conteúdos publicados são enviados através de um canal seguro; a propagação do conteúdo publicado entre servidores Friendica pode ser criptografado dependendo da configuração dos servidores; os conteúdos juntamente com suas políticas de privacidade são armazenados sem criptografia no banco de dados dos servidores Friendica.

- Atualização de Política de Privacidade - usuários podem alterar a composição dos seus grupos adicionando ou removendo membros na lista de controle de acesso dos grupos; um novo membro de um grupo poderá acessar conteúdos futuros e antigos do grupo; um usuário removido de um grupo não pode acessar conteúdos futuros porém pode acessar os conteúdos antigos já publicados pois usuários autorizados a acessar o conteúdo tem permissões permanentes; o proprietário do conteúdo já publicado não pode mais alterar a política de privacidade atribuída ao conteúdo, caso necessite de restringir o acesso a alguém que o tinha anteriormente, se sugere a exclusão do conteúdo.

Além disso, o Friendica possui grande parte das funcionalidades hoje presentes nas principais plataformas de redes sociais, facilitando o uso análogo por novos usuários. No Friendica é possível: marcar usuários e grupos por meio de "menções @"; enviar mensagens diretas; curtir ; cutucar ; usar hashtags; criar álbuns de fotografias; comentar; e compartilhar postagens visíveis publicamente.

Os principais casos de uso do software Friendica, em instância que será denominada CICFriend, no âmbito do projeto SmartUnB.ECOS são:

- Comunicação informal: O ambiente universitário gera diversas oportunidades de conexão - criação de grupos de comunicação das disciplinas do semestre, publicação de oportunidades de carreira, divulgação de disponibilidade ou necessidade de livros, criação de grupos de estudos para interesses em comum, dentre diversas outras. A utilização de uma plataforma institucional permite a personalização de serviços para melhor atender a comunidade acadêmica.

- Cutucadas em destaque: Utilizadas para abrir a comunicação entre usuários das diferentes esferas de serviço (pedagógico, administrativo, de suporte, etc), podem ser personalizadas para atingirem objetivos específicos. Por exemplo, cutucar um especialista para pedir tutoria, cutucar um orientador sobre possibilidade de orientação, cutucar colega sobre parceria em trabalho, cutucar usuários sobre proximidade de prazos.

- Projeto de inferência: Usuários podem autorizar que o sistema realize uma análise de suas participações e, com isso, o sistema poderia: atribuir acreditações por mérito, aumentar possibilidades de feedback, personalizar mais extensamente conteúdos que sejam de maior interesse do usuário, dentre outras possibilidades cogitadas a partir das contribuições da comunidade de Inteligência Artificial na Educação.

3.2 Lei Geral de Proteção de Dados - LGPD

A Lei Geral de Proteção de Dados (LGPD) foi aprovada dia 14 de agosto de 2018, entrou em vigor 24 meses após sua aprovação com sanções em vigor a partir do dia 1 de agosto de 2021 [9], e tem objetivo de se adequar às diretivas da GDPR (*General Data Protection Regulation* - Regulamento Geral de Proteção de Dados) e construir uma soberania legal sobre os dados de cidadãos e residentes do Brasil [41]. Essa lei visa proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural [42] e estabelece como fundamentos para a proteção de dados pessoais [9]:

- O respeito à privacidade;
- A autodeterminação informativa;
- A liberdade de expressão, de informação, de comunicação e de opinião;
- A inviolabilidade da intimidade, da honra e da imagem;
- O desenvolvimento econômico e tecnológico e a inovação;
- A livre iniciativa, a livre concorrência e a defesa do consumidor; e
- Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A LGPD [9] regulamenta as operações de tratamento de dados realizadas em território nacional, o tratamento de dados que tenham por objetivo a oferta ou fornecimento de

bens ou serviços ofertados em território nacional, o tratamento de dados de indivíduos localizados no território nacional ou dados pessoais que foram coletados no território nacional, seja por pessoa natural ou por pessoa jurídica de direito público ou privado.

As atividades de tratamento de dados são definidas como: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O titular é definido como pessoa natural a quem se referem os dados pessoais objetos de tratamento, e o controlador é definido como pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

E define que as atividades de tratamento de dados pessoais deverão seguir os seguintes princípios:

1. Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

2. Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

3. Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

4. Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

5. Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

6. Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

7. Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

8. Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

9. Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

10. Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

A LGPD define também o direito do titular ao acesso às informações sobre o tratamento de seus dados que deverão ser disponibilizadas de forma clara, adequada e ostensiva para o atendimento do princípio do livre acesso, dentre outras características previstas em regulamentação.

(i) - finalidade específica do tratamento;

(ii) - forma e duração do tratamento, observados os segredos comercial e industrial;

(iii) - identificação do controlador;

(iv) - informações de contato do controlador;

(v) - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

(vi) - responsabilidades dos agentes que realizarão o tratamento; e

(vii) - direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD.

Visto que essas informações têm que estar disponíveis a consulta, são informações essenciais para estarem contidas no Termo de Uso.

O artigo 18 prevê que o titular tem direito de obter do controlador, a qualquer momento e mediante requisição:

(i) - confirmação da existência de tratamento;

(ii) - acesso aos dados;

(iii) - correção de dados incompletos, inexatos ou desatualizados;

(iv) - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

(v) - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

(vi) - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

(vii) - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

(viii) - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

(ix) - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

(x) - revogação do consentimento, nos termos do inciso 5º do art. 8º desta Lei.

Além dos direitos dos usuários (titulares), a Lei Geral de Proteção de Dados elenca, em seu artigo 7º, as hipóteses em que seria admitido o tratamento de dados pessoais. Dentre elas, o inciso I determina que o tratamento de dados somente poderá ser realizado mediante o consentimento de seu titular. O pedido de consentimento além de ser obrigação legal é uma prática moral que demonstra comprometimento na relação de confiança entre usuário e provedor de um serviço.

O consentimento deve ser fornecido por escrito ou por outro meio que evidencie a manifestação de vontade do titular, deve se referir a finalidades determinadas e deve ser manifestamente expresso, livre, específico, informado, inequívoco e explícito. Será vedado o tratamento de dados pessoais mediante vício do consentimento e, em caso de autorizações genéricas, recairá a nulidade ao tratamento realizado.

O consentimento deverá ser livre, evitando práticas abusivas, de modo que o usuário não poderá ser forçado a consentir com o tratamento de seus dados. O consentimento deverá ser específico, portanto, no Termo de Uso deverá constar o objeto, o dado que se pretende tratar, bem como as finalidades referentes ao seu tratamento. O consentimento deverá ser informado, o que gera a necessidade de uma descrição rigorosa e facilmente compreensível do objeto do consentimento, das consequências do consentimento, como também de sua recusa. O consentimento deverá ser inequívoco, isto é, não deve haver espaço para dúvidas de que o titular pretendia comunicar a sua permissão para o tratamento dos seus dados. O consentimento deverá ser explícito, ou seja, deverá ser uma ação facilmente visualizável, antagonizando o consentimento deduzido pelas circunstâncias [43].

3.3 A Privacidade e o Consentimento informado

De acordo com Alan Westin [44], a privacidade é o direito de um indivíduo de determinar por si mesmo quando, como e o quanto de informações pessoais são comunicadas a terceiros. A abordagem à privacidade sob a ótica de controle não pressupõe que a informação esteja ausente nas mentes dos outros, mas que podemos determinar quem pode acessar as informações sobre nós e limitar a quem e em que condições elas são divulgadas.

A privacidade como controle foca na escolha individual e trata suas informações como parte integrante do ser. Ao reconhecer que os indivíduos têm o direito de escolher como os outros podem acessar e usar suas informações, esta perspectiva de privacidade avança a ideia de que a informação "flui naturalmente da individualidade"[45], assim, "todo homem tem uma propriedade em sua própria pessoa"e essa propriedade deve ser respeitada como sendo parte integrante de si mesmo [46]. Existem diversas teorias sobre privacidade, além da abordagem tipológica de Westin, abordadas extensivamente por Mansur [47] que não são do escopo desse estudo.

Conforme citado no Capítulo 2, o desenvolvimento da IA e sua junção com o Big Data (processamento de grandes volumes de dados) apresentam problemas únicos que estão dissolvendo o controle sobre informações pessoais. Muitas práticas de Big Data visam capturar o máximo possível da experiência humana, incluindo atividades físicas, mentais e emocionais. Ao fazer isso, indivíduos são retirados de um todo corpóreo e transformados em código binário com o objetivo de se tornarem mais móveis e comparáveis [46]. Na educação esses dados são usados para: criação de perfis de alunos para prever comportamentos como risco de abandono escolar; sistemas inteligentes que visam rastrear e moldar os hábitos de aprendizagem dos alunos; e plataformas comunitárias que rastreiam e facilitam o compartilhamento de práticas por educadores [35].

Quando comparados aos dados biomédicos, os dados coletados por tecnologias educacionais são considerados de baixo risco. Porém, com o aumento da aprendizagem mediada por computador, em que grande parte das atividades de aprendizado são realizadas através de sistemas computacionais, e as práticas de Big Data que viabilizam agregar, analisar e integrar dados de múltiplas fontes, os riscos à privacidade dos alunos aumentam, e, consequentemente, o risco da coleta de dados.

As legislações de proteção de dados em efeito hoje no mundo lidam com o consentimento informado como a principal maneira de obter autorização para o tratamento de dados pessoais. Porém estudos realizados sobre consentimento revelam que indivíduos muitas vezes não leem ou não entendem as condições com as quais concordam, seja para a participação em pesquisas ou para obter acesso a um aplicativo online. A combinação da compreensão limitada dos riscos de compartilhamento de dados e da habituação podem contribuir para que o consentimento seja dado de maneira contrária aos melhores

interesses dos participantes. A habituação comportamental é uma diminuição progressiva de resposta a um estímulo repetitivo, resultado do acúmulo de experiências anteriores de um indivíduo e traz à tona a possibilidade de que experiências relacionadas ao consentimento tenham contribuído para aumentar os níveis de apatia relacionadas às decisões de compartilhamento de dados [35].

A proliferação do uso de redes sociais e o surgimento da Internet das Coisas contribuíram para o nível de apatia relacionado à perda de privacidade e vigilância em massa. O compartilhamento de dados privados, incluindo dados biométricos, tornou-se normalizado. Assim, o risco não é apenas que os alunos se habituem a subestimar o processo de consentimento, mas também se tornem cada vez mais complacentes com os dados pessoais que são coletados e as recomendações resultantes feitas por sistemas artificialmente inteligentes. É importante ressaltar que a habituação e a complacência no aceite à recomendações realizados por sistemas de IA pode afetar também a autonomia humana, diminuindo as oportunidades de questionamento e pensamento crítico, considerada uma das habilidade essenciais da era digital.A adoção mais ampla de práticas de análise de aprendizagem como ambientes de aprendizagem adaptativos e personalizados; e abordagens de aprendizagem móvel e ubíqua podem contribuir para aumentar esse risco mencionado [35].

Instituições educacionais, educadores e pesquisadores criam e avaliam regularmente experiências formativas para alunos, com e sem o uso de tecnologia. Em situações que exigem que os alunos consentam em compartilhar seus dados, a falta de instrução em como tomar decisões informadas sobre o compartilhamento de dados pessoais pode levar alunos a atuarem contra seus próprios interesses, e a falta de treinamento de pesquisadores/professores em gerenciamento responsável de dados estudantis aumentam os riscos potenciais à proteção de dados. Preparar anteriormente os alunos/participantes para tomarem decisões informadas sobre compartilhamento de dados e abordar a importância da leitura e compreensão dos termos antes do consentimento aumenta a confiança dos alunos na tomada de decisões e na instituição [48].

Além de aumentar a instrução dos alunos e professores sobre responsabilidades e riscos no compartilhamento de dados, estudos apontam que o uso de formulários de consentimento aprimorados levam a um aumento significativo na sua compreensão [49]. A Tabela 3.1, baseada no trabalho de Beardsley [48] e adicionada de referencias da psicologia e computação, apresenta recomendações para aumentar as chances de leitura e compreensão de formulários de consentimento,

Item	Sugestão	Referências
Reduzir o nível de leitura obrigatório	Almeje um nível de leitura abaixo do 9º ano e use verificadores de legibilidade para estima-lo	[50] [51] [52] [48] [53]
Usar linguagem simples	Modifique o vocabulário utilizado, tornando-o mais familiar, curto e fácil de visualizar	[52] [51] [54] [50] [55] [56] [57] [48]
Usar sentenças curtas e simples	Divida frases longas que contêm várias ideias em frases mais curtas que contêm apenas uma.	[50] [51] [54] [55] [48]
Diminuir blocos de textos e explicações	Mantenha o comprimento do parágrafo abaixo de sete linhas.	[57] [54] [50] [58] [52] [48]
Títulos de seção em negrito	Descreva as informações sobre os tipos de dados em um parágrafo separado, sob um cabeçalho separado, para atrair a atenção adequada	[54] [58] [59] [48]
Incluir listas com marcadores e resumos	Use marcadores para separar longas explicações	[55] [58] [50] [60] [59] [48]
Utilizar mais espaços brancos e aumentar o espaçamento entre linhas	Aumentar espaços brancos para tornar os formulários mais legíveis	[55] [52] [48]
Organizar informações baseada na relevância para o leitor	Reestruture as informações em uma sequência que seja lógica do ponto de vista do receptor	[51] [61] [60] [56] [62] [63] [48]
Diminuir ao máximo o texto	Elaborar texto com até 200 palavras para manter tempo requerido de leitura abaixo de 1 minuto	[64] [53]
Adicionar elementos interativos e ilustrativos	Adicionar elementos interativos como pop-ups com principais pontos e questões sobre o formulário, e imagens para reter atenção do participante	[53] [64] [57]

Tabela 3.1: Recomendações para aprimorar formulários de consentimento baseadas na literatura

3.4 Desafios e *framework* ético para guiar projeto em tecnologia educacional

O uso da tecnologia em ambientes educacionais e para a educação está em crescimento exponencial, especialmente após a pandemia de Covid-19, que se iniciou em 2019 e se espalhou rapidamente pelo mundo, gerando restrições de circulação e convivência entre pessoas, acelerando a adoção de meios virtuais para a continuação do ensino.

Com o aumento do aprendizado mediado por computadores, uma quantidade massiva de dados está sendo gerada sobre diversos aspectos envolvidos na aprendizagem. Essas trilhas de dados produzidas pelos alunos fornecem informações valiosas sobre o que está

acontecendo no processo de aprendizagem e podem sugerir maneiras pelas quais os educadores podem fazer melhorias [65]. Pesquisadores da área de *Learning Analytics* afirmam que o acesso e a análise de dados educacionais melhorará a qualidade e o valor da experiência de aprendizagem, apoiará a aprendizagem autorregulada, ajudará a identificar como a aprendizagem e os serviços aos alunos podem ser melhorados e ajudará os alunos em risco de falhar [36].

Porém as implicações éticas para o uso de dados estudantis e dessas novas tecnologias são as mais diversas, desde questões de privacidade e propriedade de dados até questões mais subjetiva como o significado de sucesso do aluno.

No Capítulo 2, em sua última seção - Pauta mais recente: projeto e utilização, são citados estudos que abordam implicações éticas da *Learning Analytics*. Uma revisão desses estudos foi realizada, adicionando a contribuição de Ferguson [66], Os desafios ético encontrados foram então listados e subsequentemente categorizados de acordo com as Questões Centrais propostas por Slade e Tait [29], nas diretrizes globais para ética em *Learning Analytics*:

Questão 1: Propriedade e controle de dados - Desafios quanto à de quem pertence os dados e o controle que os alunos podem ter quanto ao uso de seus dados;

- Detalhar os proprietários dos diferentes tipos de dados educacionais [31] [66];
- Cumprir a lei [66] [29];
- Garantir segurança dos dados [27] [66];
- Permitir a manutenção da divisão entre vida (e dados) pública e privada no contexto das relações assimétricas de poder na educação [27] [8] [66];
- Unificar o conjunto de diretrizes relacionadas ao uso ético de dados em toda a gama de serviços digitais usados [26] [31];
- Em relação a dados pessoais e confidenciais, os alunos devem ter opções para determinar quais dados podem ser coletados, como esses dados podem ser usados, quem pode acessar-los e para quais fins [29];
- Instituições devem conceder aos alunos a capacidade de corrigir e/ou adicionar contexto aos seus dados brutos, e de revisar e se contrapor a escolhas que parecem ser limitadas como resultado de um aplicativo de análise de aprendizagem [26] [27] [29];
- Procedimentos de gerenciamento de dados claramente delineados, que incluem a limitação do tempo para o qual o consentimento é válido e de armazenamento de dados, e procedimentos para sua destruição ou anonimização [26] [27] [66] [34];
- A identidade do aluno é dinâmica, os alunos devem poder evoluir de experiências anteriores sem que essas experiências se tornem manchas permanentes em seu histórico de desenvolvimento [26];

- Esclarecer a existência de qualquer possível utilização de dados para fins comerciais, seja através de terceiros ou pela comercialização da solução de *Learning Analytics* [34];
- Fornecer salvaguardas adicionais para indivíduos vulneráveis [26] [66];

Questão 2: Transparência - Desafios relacionados ao detalhamento do funcionamento das aplicações e o tratamento de dados.

- Detalhar todos os possíveis contextos em que pode ser realizado o compartilhamento de dados com terceiros [29] [66];
- Detalhar os fins para os quais os dados serão utilizados, em que condições, quem terá acesso aos dados e as medidas através das quais a identidade dos indivíduos será protegida [26] [27] [29] [31];
- Definir as partes interessadas e como cada uma se beneficia do uso da *Learning Analytics* e em que condições [26] [29];
- Ser transparente quanto aos dados que são coletados (e os que não são), , as fontes utilizadas, como são coletados, analisados e utilizados para moldar as possíveis jornadas de aprendizagem dos alunos, e quaisquer suposições feitas sobre esses dados (onde podem estar incompletos ou estarem agindo como um proxy para outra medida, por exemplo) [29] [36];
- Permitir acesso aos alunos a informações sobre suas escolhas de estudo, como e por que elas podem ser afetadas pela análise, e prover oportunidade de alterar ou corrigir o conjunto de dados (ou as interpretações obtidas a partir dele) e de adicionar ao entendimento institucional os fatores relevantes que impactam no sucesso do aluno [29];
- No caso de implementação de algoritmos de difícil interpretação, como redes neurais profundas, associar seu uso a uma técnica de explicabilidade, fazendo com que os dados e resultados sejam compreensíveis ao usuário final [26] [29] [66];

Questão 3: Acessibilidade de dados - Desafios relacionados à quem tem acesso aos dados, os meios de acesso, de os modificarem e negarem análises.

- Instituições devem esclarecer: quem tem acesso aos dados brutos e analisados dos estudantes, meios dos alunos acessarem e corrigirem seus próprios dados, quais dados usualmente são incluídos em um aplicativo de análise de aprendizagem e, caso haja categorias de dados irrelevantes ou sensíveis, que podem sempre ser considerados fora do escopo [29] [66];
- Direito do aluno de permanecer um indivíduo e considerações se é apropriado para os alunos terem conhecimento dos rótulos que lhes são atribuídos [29],

Questão 4: Validade e confiabilidade dos dados - Desafios relacionados à precisão, representatividade e limitação dos dados.

- Garantir que os dados coletados e analisados sejam precisos e representativos do problema que está sendo medido [29] [30],
- Garantir que a *Learning Analytics* leve em conta tudo que se sabe sobre ensino e aprendizagem, e considerar as limitações da coleta e processamento de dados para representar todo o processo da educação [31],
- Analisar a validade dos algoritmos e as métricas usadas para análises preditivas ou intervenções com base nos dados do aluno [36],
- Refletir sobre a possibilidade de viés algorítmico (por exemplo pelo treinamento sobre conjunto de dados não representativos, ou baseado em decisões que já continham preconceitos ou vieses) podendo levar a soluções que perpetuem, exacerbem ou mascaram discriminação prejudicial [26] [66] [31] [35];
- Refletir sobre a natureza e interpretação dos dados digitais e como não são totalmente representativos de um aluno em particular [26];
- Refletir sobre a natureza transitória dos objetivos, interesses e emoções dos alunos, e como incorporar esse conceito à prática da *Learning Analytics* [19];
- Fornecer oportunidades para o desafio das análises preditivas e para uma possível correção de dados [29];
- Garantir o uso da aplicação de forma consistente com a intenção dos designers, e estabelecer protocolos com melhores práticas para as possíveis intervenções necessárias [8];
- Primeiro considerar o que a instituição está tentando medir e como isso pode ser melhor representado (invés de examinar os dados disponíveis primeiro e descobrir como eles podem ser aplicados) [29];
- Garantir/melhorar as competências da equipe e a compreensão das complexidades e implicações éticas na coleta, análise e uso de dados dos alunos [29] [20] [31];
- Manter os conjuntos de dados atualizados tanto quanto possível, com oportunidades para que os alunos e outras partes interessadas atualizem e substituam os dados existentes [29].
- Realizar a integração de dados de diferentes fontes com cuidado [66],
- Pensar no sucesso do aluno como o resultado de "interações principalmente não lineares, multidimensionais e interdependentes em diferentes fases do nexo entre o aluno, a instituição e o fator social mais amplo"[26].

Questão 5: Responsabilidade institucional e obrigação de agir - Desafios relacionados às decisões quanto ao uso de LA, quanto a alocação de recursos, e análise do seu impacto.

- Definir se ao conhecer e compreender mais sobre como os alunos aprendem, ex. identificando probabilidade de falha do aluno traz consigo uma obrigação moral de agir [26] [29];
- O processo de tomada de decisão para identificar a alocação de recurso de suporte deve ser transparente e claramente compreendido por todas as partes interessadas [29];
- Definir circunstâncias específicas em que as instituições devem intervir devido a análises, sugerindo que os alunos poderiam se beneficiar de suporte adicional [36];
- Habilitar o uso da análise de aprendizagem não apenas no que é eficaz, mas também ter como objetivo fornecer indicadores relevantes para decidir o que é apropriado e moralmente necessário [26];
- Dados não serão tratados como uma mercadoria, e sim como uma troca entregando o suporte e serviços prometidos [31]
- O custo ético da inação e do fracasso em inovar deve ser equilibrado contra o potencial de inovação da AIED para resultar em benefícios reais para alunos, educadores, instituições educacionais e a sociedade em geral [20].
- Investigar o impacto da *Learning Analytics* na satisfação profissional do professor e definir ações para que ocorra a integração das inovações tecnológicas às técnicas pedagógicas do professor [31];

Questão 6: Comunicações - Desafios relacionados às formas de entrar em contato com alunos devido a analíticas e interpretação dos dados.

- Ter cuidado nas comunicações diretas com os alunos com base em dados analiticos, lembrar que os dados são só predições, ou seja, uma probabilidade gerada por um computador [8] [29]
- Garantir, por meio de comunicação regular, que a equipe: compreenda a abordagem - utilização de termos genéricos de suporte ao invés de termos probabilísticos: os valores subjacentes vinculados à missão e estratégia da instituição; os benefícios esperados para os alunos; as limitações dos dados e sua interpretação; e diretrizes para a prática ética. [8] [29]

Questão 7: Valores culturais - Desafios relacionados às mudanças de cultura e suas implicações em LA.

- Analisar, caso a caso, com cuidado a possibilidade de reuso de sistemas de análises de aprendizado, pois medidas previamente estabelecidas como correlacionadas com resultados bem ou malsucedidos provavelmente diferem em diferentes geografias e culturas;

- Ter cuidado no caso de compra de pacotes analíticos de desenvolvedores para garantir que a abordagem é adequada para o propósito e pode ser adaptada com dados e restrições locais em mente.

Questão 8: Inclusão - Desafios relacionados à utilização de LA de maneira inclusiva e habilitando equidade ao acesso à educação.

- Risco que a *Learning Analytics* seja usada de maneiras que legitimam a exclusão se seu uso se relacionar predominantemente ao desejo da instituição de proteger suas taxas de sucesso.
- Compartilhe *insights* e descobertas entre as divisões digitais para colaborar para equalidade de acesso à educação.

Questão 9: Consentimento - Desafios relacionados à obtenção de autorização para uso de dados, e de consentimento parcial.

- Se o consentimento for solicitado na fase de matrícula, ele deve ser acompanhado de transparência (da finalidade, dos dados coletados, etc.) e, com uma opção posterior de retirá-lo.
- Considerar a influência das relações assimétrica de poder entre instituições e alunos, e o potencial de coerção no processo de consentimento em que seu não provimento pode acarretar em prejuízo pro aluno.
- O consentimento não deve ser considerado em termos binários simples, mas apresentado aos alunos como um menu de opções que dependem da finalidade da coleta, análise e uso de seus dados, o módulo disciplinar ou contexto, a variedade de dados possíveis que podem ser coletados , analisados e usados, e uma compreensão dos riscos de optar por in / out.
- Garantir que os resultados analíticos sejam vistos e interpretados como indicadores.
- Refletir sobre a possível natureza transitória da classificação de dados como sensíveis dependendo do contexto ou momento
- Melhorar a alfabetização de dados dos alunos, provendo ferramentas que os ajudem a entender os riscos e benefícios do compartilhamento de dados, colaborando assim para o consentimento informado.
- Aumentar a compreensão de pesquisadores e desenvolvedores de análise de aprendizagem, dos processos de ensino e aprendizagem,
- Apresentar de modo simples, transparente e detalhado os dados coletados e seus propósitos, a fim de minimizar a percepção de vigilância.

Questão 10: Agência e responsabilidade do aluno - Desafios relacionados à engajar o aluno mais ativamente nos projeto de LA.

- Apresentar aos alunos, de modo claro, interessante e transparente as soluções de tecnologia educacional utilizadas no contexto acadêmico, seu funcionamento, propósito e dados coletados, para aumentar a compreensão dos alunos dos benefícios em colaborar com o sistema e assim com seu próprio aprendizado, apoiando assim a agência e autonomia dos alunos, e apoiando o processo de consentimento informado [26] [29];
- Engajar proativamente alunos no desenvolvimento e implementação da *Learning Analytics*, de maneira que os alunos estejam mais ativamente envolvidos em ajudar a instituição a projetar e moldar as intervenções que os apoiarão [26] [29].

Slade [26] propôs uma série de princípios como framework de orientação para considerar a análise da aprendizagem como prática moral. Sua abordagem afirma que o uso de análise de aprendizagem por uma instituição será baseado em sua compreensão do escopo, papel e limites da análise de aprendizagem e um conjunto de crenças morais fundadas nos respectivos contextos regulatórios e legais, culturais, geopolíticos e socioeconômicos. Os princípios a seguir devem servir como base para a criação de diretrizes institucionais baseadas no contexto.

Princípios para um framework ético para a *Learning Analytics*:

Princípio 1: Learning Analytics como prática moral

A educação não deve ser entendida como uma intervenção ou tratamento e sim como uma prática moral.

Princípio 2: Alunos como agentes

A análise de aprendizagem deve envolver os alunos como colaboradores e não como meros destinatários de intervenções e serviços. Valorizar os alunos como agentes, que fazem escolhas e colaboraram com a instituição na construção de suas identidades (embora transitórias) pode, além disso, ser um antídoto útil (e poderoso) para a comercialização do ensino superior no contexto do impacto das relações de poder distorcidas, monitoramento e vigilância.

Princípio 3: A identidade e o desempenho do aluno são construções dinâmicas temporais

Integral na análise de aprendizagem é a noção de identidade do aluno. É crucial ver a identidade do aluno como uma combinação de atributos permanentes e dinâmicos. Durante a matrícula dos alunos, suas identidades estão em fluxo contínuo, as implicações éticas disso são que a análise de aprendizagem fornece uma visão instantânea de um aluno em um determinado momento e contexto. Sendo assim os dados coletados por meio da análise de aprendizagem devem ter uma vida útil e uma data de expiração combinadas,

bem como mecanismos para que os alunos solicitem a exclusão de dados de acordo com os critérios acordados.

Princípio 4: O sucesso do aluno é um fenômeno complexo e multidimensional

Embora um dos benefícios da análise de aprendizagem seja contribuir para uma melhor compreensão da demografia e dos comportamentos dos alunos, é importante ver o sucesso do aluno como resultado de interações interdependentes, multidimensionais e não lineares entre alunos, instituição e sociedade. Embora a análise de aprendizagem ofereça grandes oportunidades para obter uma compreensão mais abrangente da aprendizagem do aluno, nossos dados são incompletos e nossas análises vulneráveis a interpretações errôneas e preconceitos.

Princípio 5: Transparência

Instituições de ensino superior devem ser transparentes em relação às finalidades para as quais os dados serão usados, sob quais condições, quem terá acesso aos dados e as medidas por meio das quais a identidade dos indivíduos serão protegidas. Além disso tem a obrigação de proteger os dados dos alunos e de informar alunos sobre possíveis riscos quando o ensino e a aprendizagem ocorrem fora dos limites da jurisdição institucional.

Princípio 6: O ensino superior não pode se dar ao luxo de não usar dados

As instituições são responsáveis, independentemente do gatilho utilizado para a adoção da análise de aprendizagem, de usar os dados disponíveis para entender melhor e, em seguida, se envolver e, de fato, melhorar os resultados. Ignorar informações que possam ajudar ativamente a perseguir os objetivos de uma instituição parece uma visão limitada.

Capítulo 4

Proposta: Contribuições para tecnologia educacional eticamente consciente à luz da CICFriend

Neste capítulo serão apresentados os artefatos e suas construções. Com base em cada uma das seções abaixo será possível generalizar as recomendações dadas para a construção de artefatos para outros sistemas que realizem o tratamento de dados pessoais. Na primeira seção se encontra todos os dados que precisam constar em um Termo de Uso e em uma Política de Privacidade aderente à LGPD, além de apresentar a Declaração de Privacidade e seu intuito. Na segunda seção se encontra os fundamentos para a construção da matriz de riscos e benefícios, e como ela pode ser utilizada para clarificar potenciais riscos operacionais e éticos no tratamento de dados pessoais. Na terceira seção são fornecidas, de acordo com a literatura, recomendações para a criação de um Termo de Consentimento Livre e Esclarecido que esteja em conformidade com as resoluções normativas e que colabore para o consentimento informado.

4.1 Quanto a Implantação: Termo de Uso, Política de Privacidade e a Declaração de Privacidade

O Termo de Uso, Termo de Serviço ou Contrato de Termo de Uso é um documento que estabelece as condições e as regras de uso de determinado serviço. O aceite do Termo de Uso vincula a utilização do serviço às clausulas do termo. A Política de Privacidade é um documento informativo em que o prestador de serviço explica ao usuário como será feito o tratamento dos dados pessoais e como será fornecida privacidade [67].

Tanto o Termo de Uso quanto a Política de Privacidade surgem da responsabilidade de transparência no relacionamento entre os agentes de tratamento de dados com o titular dos dados e de informar como as atividades de tratamento de dados atendem os princípios dispostos no artigo 6º da Lei Geral de Proteção de Dados Pessoais (LGPD) [9]. Portanto, os dois documentos constituem, ao mesmo tempo, um dever do controlador e um direito do titular [67].

O Ministério da Economia disponibilizou uma série de guias operacionais para adequação à LGPD com o intuito de incentivar a cultura de proteção de dados e acelerar a evolução da maturidade necessária para que órgãos e entidades federais possam ter conformidade à Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

O guia governamental sugere a inclusão dos seguintes tópicos contendo respectivas informações importantes para a elaboração do Termo de Uso:

1. Aceitação dos termos e políticas

   Termos e políticas do aplicativo aplicáveis e que o uso do serviço expressa acordo com os Termos apresentados.

2. Definições

   Definições necessárias sobre os termos utilizados no documento, incluindo os da Lei Geral de Proteção de Dados.

3. Arcabouço Legal

   Leis e normativos que podem ser consultados pelo titular para esclarecimento de dúvidas e o arcabouço jurídico que respalda o tratamento de dados pessoais;

4. Descrição de serviço

   Informações sobre quem é o responsável pela prestação do serviço, descrição do escopo do serviço e sua finalidade; forma de utilização do serviço e informações necessárias para seu uso adequado.

5. Direitos do usuário

   Os direitos detalhados do titular que utiliza o serviço.

6. Responsabilidades do usuário e da Administração Pública (provedor do serviço)

   Limitação da responsabilidade da administração e excludentes de responsabilidade; e responsabilidades do usuário ao utilizar o serviço.

7. Mudanças no Termo de Uso

   Como as alterações no Termo de Uso serão comunicadas.

8. Informações para contato

   Os canais para esclarecimento de dúvidas e detalhes sobre seu funcionamento.

9. Foro

   Quem será responsável por receber eventuais litígios e o direito do titular para reclamar à Autoridade Nacional de Proteção de Dados.

A Política de Privacidade tem como objetivo descrever ao usuário o método, os processos e os procedimentos adotados no tratamento de dados pessoais pelo serviço e informá-lo sobre as medidas de privacidade empregadas. De acordo com o Serviço Federal de Processamento de Dados (SERPRO) [68] e o Guia de Elaboração de Termo de Uso e política de Privacidade para serviços públicos, a política de Privacidade tem que conter as seguintes informações:

1. Informações sobre a organização responsável pelo tratamento;

   Identificação, endereço e informações de contato do controlador; caso o operador seja diferente do controlador identificação e endereço do controlador; caso tenha sido definido um Encarregado: identificação e informações de contato do encarregado.

2. Informações sobre o tratamento de dados;

   Dados pessoais coletados inclusive os não informados pelo usuário (exemplo: IP, localização, etc); como são coletados, quais as operações de tratamento realizadas em cada tipo de dados e suas respectivas finalidades, e o prazo de retenção dos mesmos;

3. Compartilhamento de dados

   Quais dados são compartilhados, com quem e qual a finalidade do compartilhamento.

4. Segurança

   Medidas de segurança implementadas no serviço e informar ao titular que incidentes de segurança que possam acarretar risco ou dano relevante aos titulares serão comunicados.

5. Cookies

Informações sobre o uso de cookies (proprietários e de terceiros), os dados coletados, sua finalidade e como obter mais informações sobre os cookies de terceiros utilizados no serviço.

6. Tratamento posterior para outras finalidades

   Informação dos dados que poderão ser utilizados para tratamentos posteriores e a finalidades deste tratamento;

7. Transferência Internacional de Dados

   Quais dados transferidos, qual a finalidade da transferência, quais países envolvidos e respectivo grau de proteção de dados pessoais fornecido;

8. Decisões automatizadas

   Quais decisões podem ser tomadas em quais circunstâncias.

Vale ressaltar que o guia citado é elaborado para órgãos e entidades da Administração Pública Federal direta, e que as Universidades públicas estão inclusas na administração pública indireta com estatuto jurídico especial [69], o que não invalida porém suas recomendações.

Com base nesses guias, nos Termos de Uso e Política de Privacidade da instância Venera Social do Friendica, nos Termos de Uso e Políticas de Privacidade dos ambientes do Aprender UnB, nos Termos de Uso e Políticas de Privacidade da rede social Facebook, na Lei vigente, e na literatura, foram propostos no Apêndice A os artefatos: Declaração de Privacidade, Termo de Uso e Política de Privacidade.

A declaração de privacidade foi elaborada com o objetivo de cumprir o papel de apoiar o consentimento informado, visto que, conforme mostrado na seção sobre Privacidade e Consentimento Informado, existem diversos estudos que indicam a não leitura e a habituação ao consentimento.

Para isso foi elaborado um texto simples, seguindo as recomendações da Tabela 3.1: Texto com nível de leitura abaixo do público alvo (estudantes universitários), linguagem simples, sentenças e parágrafos curtos, organizado em tópicos, com uso de espaçamento grande, orientado ao participante e com menos de 200 palavras. O nível de leitura foi calculado através do Índices de Legibilidade de Flesch-Kincaid, cuja validade para o português já foi atestada em diversas publicações [70].

É proposto que esse texto seja apresentado ao usuário de maneira visualmente atrativa e que a opção para inscrição seja colocada ao fim do texto.

O Termo de Uso e a Política de Privacidade propostos foram elaborados seguindo os requisitos da LGPD, as recomendações listadas acima e de acordo com as especificidades

do software Friendica. Devido aos requisitos legais estes textos são extensos, porém as recomendações propostas foram seguidas quando possível, mantendo o texto com sentenças e parágrafos curtos e organizado em tópicos.

É proposto que esses documentos sejam apresentados ao usuário de maneira interativa de maneira que seja possível navegar entre os tópicos abordados independentemente.

4.2 Quanto ao Projeto e Desenvolvimento: Mapa de benefícios e riscos

Para apoiar no projeto e desenvolvimento ético de tecnologias educacionais, é proposta uma matriz de riscos e benefícios relacionada às operações de tratamento de dados. Esta proposta se embasa na: importância de se considerar o uso ético de dados de alunos, sujeito de diversos dos desafios éticos citados no Capítulo 3; importância de se estabelecer boas práticas de governança de dados e privacidade; para demonstrar, seguindo o princípio de transparência e consentimento informado, os riscos, éticos e operacionais, e benefícios envolvendo o compartilhamento de dados; e demonstrar conformidade com a legislação.

A matriz preenchida como exemplo considerando as especificidades do caso de uso do CICFriend está presente no Apêndice B. A Figura 4.1 apresenta a matriz sem o preenchimento, somente com a descrição e as perguntas orientadoras a serem preenchidas pelos desenvolvedores e projetistas de novas aplicações.

A formalização dos riscos e benefícios do tratamento de dados apoiará também a construção do Termo de Consentimento Livre e Esclarecido (TCLE) e do Termo de Uso, de modo que todos usuários e futuros participantes de pesquisa estejam cientes dos riscos e benefícios envolvidos.

A construção da matriz se constitui em linhas contendo o tipo de tratamento a ser analisado, e colunas de riscos, mitigações, benefícios, descrição e perguntas orientadoras. Os tipos de tratamento considerados são as fases do ciclo de vida do tratamento de dados pessoais [71]: coleta, armazenamento, processamento, apresentação e compartilhamento. Essas categorias se relacionam com as operações de tratamento da LGPD de acordo com a Tabela 3.1.

A operação de tratamento “acesso” (LGPD, art. 5º, X) está presente em todas as fases do ciclo de vida dos dados pessoais, pois de alguma forma temos que realizar acesso ao dado pessoal para viabilizar sua coleta, retenção, processamento, compartilhamento ou eliminação.

A norma ISO/IEC 29134:2017 fornece diretrizes para a realização de processos de avaliação de impacto de privacidade, e a estrutura e o conteúdo de relatório de avaliação de impacto de privacidade. Na sua seção 6.4.4. é fornecida uma lista exaustiva de riscos

Tipo tratamento	Riscos	Mitigações	Benefícios	Descrição	Perguntas Orientadoras
Coleta de dados	Preencher a partir das perguntas orientadoras	Quais são os passos tomados para mitigar os riscos?	Quais os benefícios para os stakeholders que compensem possíveis riscos?	Avaliar riscos éticos e operacionais da etapa de coleta (operações de coleta, produção e recepção) de dados, especialmente os que tratam dos princípios de: transparência, consentimento informado e agência e responsabilidade do aluno.	Quais os riscos do fornecimento de dados inválidos? Quais os riscos da falta informações levar a um consentimento inválido? Quais os riscos do não engajamento com alunos? Quais os riscos de acesso não autorizado? Quais os riscos da coleção excessiva de dados?
Retenção				Avaliar riscos éticos e operacionais na retenção (arquivamento e armazenamento) de dados, especialmente os que tratam dos princípios de: transparência, propriedade e controle de dados e acessibilidade.	Quais os riscos de acesso não autorizado? Quais os riscos de perda de dados? Quais os riscos inerentes do procedimentos para cumprir os prazos de retenção de dados? Quais os dados passíveis de anonimização? Quais dados podem ter tratamentos posteriores? Todos essas possibilidades foram informadas?
Processamento				Avaliar riscos éticos e operacionais do processamento de dados, especialmente os que tratam dos princípios de: transparência, propriedade e controle de dados, validade e confiabilidade dos dados, responsabilidade institucional e obrigação de agir, valores culturais, inclusão e consentimento	Quais os riscos de uma classificação/agrupamento enviesado? Quais os riscos de processamento de dados sensíveis? Quais os riscos de reuso não informado? Quais os riscos de tratar os dados mais que o comunicado (transparência)? Quais os riscos de não agir sobre informação? Quais os riscos da extrapolação de dados? Quais os riscos de viés? Quais os riscos da avaliação levar à exclusão? Quais os riscos de modificação não autorizada? Quais os riscos de falha ou erro de processamento?
Compartilhamento				Avaliar riscos éticos e operacionais do compartilhamento de dados, especialmente os que tratam dos princípios de: transparência, propriedade e controle de dados e acessibilidade, validade e confiabilidade dos dados, comunicações e consentimento.	Quais os riscos de acesso indevido? Quais os riscos de compartilhamento de análises que são estatísticas? Quais os riscos de comunicação indevida como resultado de análises? Quais os riscos de compartilhamento além do consentido?
Eliminação				Avaliar riscos éticos e operacionais da eliminação de dados, especialmente os que tratam dos princípios de: transparência, propriedade e controle de dados e consentimento.	Quais os riscos na eliminação indevida de dados? Quais os riscos de perda de dados? Quais os riscos na anonimização de dados antes da eliminação para fins de reuso? Quais os risco de reidentificação de dados anonimizados? Quais os riscos sobre o direito de saber do tratamento de dados ocorrido?

Figura 4.1: Matriz de riscos e benefícios.

operacionais de privacidade e de segurança, que será apresentada abaixo para colaborar na identificação de riscos no tratamento de dados pessoais.

- Acesso não autorizado.
- Modificação não autorizada.
- Perda.

Fase do ciclo de tratamento	**Operações de tratamento da LGPD**
Coleta	Coleta, produção, recepção
Retenção	Arquivamento e armazenamento
Processamento	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação.
Compartilhamento	Transmissão, distribuição, comunicação, transferência e difusão.
Eliminação	Eliminação

Tabela 4.1: Fases do ciclo de vida e respectivas operações de tratamento

- Roubo.
- Remoção não autorizada.
- Coleção excessiva.
- Informação insuficiente sobre a finalidade do tratamento.
- Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).
- Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).
- Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.
- Retenção prolongada de dados pessoais sem necessidade.
- Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.
- Falha ou erro de processamento (Ex.: execução de *script* de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada, etc.).
- Reidentificação de dados pseudonimizados.

Para avaliar os riscos éticos no tratamento de dados será novamente utilizada a categorização proposta por Slade, que divide os problemas éticos em 10 Questões Centrais, que serão analisadas sob a ótica de cada momento do ciclo de vida do tratamento de dados.

1. Transparência
2. Propriedade e controle de dados
3. Acessibilidade de dados
4. Validade e confiabilidade dos dados
5. Responsabilidade institucional e obrigação de agir
6. Comunicações
7. Valores culturais
8. Inclusão

9. Consentimento
10. Agência e responsabilidade do aluno

4.3 Quanto a Avaliação: TCLE

O Termo de Consentimento Livre e Esclarecido (TCLE) é um documento requisito para a submissão de um projeto de pesquisa envolvendo humanos. No âmbito do projeto CICFriend, a pesquisa será realizada com usuários dessa plataforma, com o objetivo de avaliar a percepção inicial dos usuários em relação a rede social e as suas interações com a mesma.

A pesquisa será realizada em três momentos:

1. Aplicação de questionário sobre utilização de redes sociais;

2. Coleta de dados da aplicação CICFriend para mensurar as interações ocorridas durante seu uso;

3. Reunião com um grupo focal para debate sobre os benefícios e a validade do uso do serviço no contexto educacional.

A Resolução número 510 de 2016 do Conselho Nacional de Saúde, em seu Capítulo I, Artigo 2, XXII [23], define:

"registro do consentimento ou do assentimento": documento em qualquer meio, formato ou mídia, como papel, áudio, filmagem, mídia eletrônica e digital, que registra a concessão de consentimento ou de assentimento livre e esclarecido, sendo a forma de registro escolhida a partir das características individuais, sociais, linguísticas, econômicas e culturais do participante da pesquisa e em razão das abordagens metodológicas aplicadas.

Sendo assim, o uso de um TCLE digital segue as mesmas regras, devendo conter todas as informações que serão descritas a seguir, porém visto a praticidade e agilidade disponibilizada pela tecnologia, novos formatos podem ser utilizados.

Para a construção de um TCLE que contemple as determinações das resoluções vigentes, de acordo com as referências fornecidas no Capítulo 2, e colabore para aumentar o índice de leitura e compreensão, requisitos para o consentimento informado, de acordo com as referências fornecidas no Capítulo 3, as recomendações a seguir foram seguidas:

1. Utilizar linguagem simples, acessível e amigável em todo o documento, visando um nível de leitura de ensino médio para garantir inclusividade, dado que o público-alvo são estudantes universitários. Usar marcadores quando possível para facilitar a visualização dos dados. Usar preferencialmente a forma de tratamento "você". Em caso de TCLE Digital: Informar ao participante o tempo previsto para o cumprimento

da etapa de pesquisa específica, como, por exemplo, o tempo médio para responder questionário. E na medida do possível, deve ser dada a possibilidade de interromper tal ação, "salvando" o que foi feito para continuar assim que possível, ou desistir da participação, se assim desejar.

2. Iniciar o documento com: nome do pesquisador; sua vinculação acadêmica (curso, instituição, orientador etc); o título da pesquisa (conforme registro na Plataforma Brasil e no seu projeto completo); o objetivo principal e a justificativa do estudo.

3. Descrever como será desenvolvida a pesquisa (procedimentos metodológicos): listar os passos e instrumentos utilizados para a geração dos dados, como entrevista, questionário ou outros meios. No caso de serem utilizadas fotografias, gravações em áudio e vídeo informar ao participante de maneira clara e destacada essa necessidade e o destino que será dado a esse material.

4. Informar a garantia de confidencialidade das informações, da privacidade do participante e da proteção da sua identidade inclusive do uso da sua imagem e voz. Informe que:

   (i) não serão divulgados nomes ou informações que possam identificar os envolvidos na pesquisa ou local(is) onde a pesquisa vai se desenvolver;

   (ii) os dados obtidos serão utilizados apenas para fins de estudo;

   (iii) o participante pode desistir do estudo a qualquer momento, sem prejuízo de qualquer natureza, em caso de desistência, os dados coletados do participante serão removidos;

   (iv) o participante pode obter informações quanto ao andamento do estudo fazendo contato pelo e-mail e/ou telefone do(s) responsável(eis) pela pesquisa (esses dados devem ser escritos no texto);

   (v) a devolutiva será realizada e de que forma;

   (vi) a pesquisa apresenta riscos (de gradação mínima, baixa, moderada ou elevada), danos, desconfortos, exemplificando-os e indicando respectivas medidas de proteção ao participante, quando pertinente;

   (vii) a participação possui também benefícios e quais são;

   (viii) Em caso de TCLE impresso: uma via ficará em posse do participante, e a outra sob sua responsabilidade ou da equipe de pesquisa. Em caso de TCLE digital: o consentimento consta ou na assinatura digital, ou no preenchimento do campo de aceite no formulário ou na simples devolução do formulário (deve estar definido e especificado nesse documento).

5. Em caso de TCLE Impresso: Inserir dois campos reservados para as assinaturas: do participante do estudo, se maior de 18 anos ou do seu responsável caso contrário; e do responsável pela pesquisa (aluno/a/Mestre/Doutor/a) ou orientador (no caso de Trabalho de Conclusão de Curso (TCC)).

A Resolução n. 466/12 também orienta que: os espaços para as assinaturas estejam na mesma página; e as páginas que não apresentarem campos de assinaturas precisam ser rubricadas pelo pesquisador e pelo participante ou seu responsável.

Em caso de TCLE Digital o modo de confirmação de participação na pesquisa (assinatura digital, campo de aceite ou apenas a submissão do questionário), deve estar claro tanto no TCLE quanto nos esclarecimentos éticos do projeto de pesquisa. Caso seja necessário, o pesquisador deve orientar os participantes quanto às especificações técnicas necessárias para que os dados sejam obtidos com sucesso, como por exemplo, caso a ferramenta utilizada funcione melhor em algum navegador específico.

O pesquisador deve ter acesso e se responsabilizar pelas informações referentes a seus participantes no que diz respeito aos dados on-line e aos dados físicos, pesquisador é responsável por uma das vias do documento.

Capítulo 5

Conclusão

Este capítulo apresenta as ideias conclusivas deste trabalho e possibilidades de trabalhos futuros.

5.1 Objetivos alcançados

O aumento do uso da tecnologia na educação para a manutenção das atividades educacionais durante a pandemia de Covid-19, e a quantidade massiva de dados gerados das interações entre professores, alunos e seus ambientes virtuais de ensino gerou um campo fértil para a aplicação de *Learning Analytics*, sistemas que coletam, analisam e relatam dados sobre os alunos para otimizar a aprendizagem. Esses sistemas utilizam técnicas computacionais associadas a grandes quantidades de dados educacionais para realizar analises preditivas sobre as mais diversas formas de aumentar o desempenho estudantil, desde analises de técnicas pedagógicas mais eficazes até do risco de falha de um aluno. As implicações éticas do uso de dados estudantis, muitas vezes sem consentimento informado, foi um dos motivadores deste trabalho.

Para aprofundar o entendimento sobre ética em *Learning Analytics*, uma revisão de literatura em linha de tempo foi realizada, e os desafios éticos encontrados nas publicações referenciadas foram então listados e categorizados dentre questões pertinentes à: transparência, posse e controle de dados, acessibilidade de dados, validade e confiabilidade dos dados, responsabilidade institucional e obrigação de agir, comunicações, valores culturais, inclusão, consentimento, e agência e responsabilidade do aluno. Mais de 100 desafios foram identificados, estes foram então compilados, listados, redundâncias foram consolidadas, e um novo entendimento sobre ética em *Learning Analytics* foi alcançado.

O objetivo geral desta pesquisa era prover ferramentas práticas para apoiar no desenvolvimento ético, não só no contexto do projeto CICFriend e mais amplamente do

SmartUnB.ECOS, mas para quaisquer projetos de tecnologia que envolvam o tratamento de dados pessoais. Para tal, foram fornecidas:

1. Recomendações para o desenvolvimento de formulários de consentimento;
2. Recomendações e requisitos para a elaboração de um Termo de Uso;
3. Recomendações e requisitos para a elaboração de uma Política de Privacidade;
4. Recomendações para a elaboração de um Termo de Consentimento Livre e Esclarecido;
5. Matriz de Riscos e Benefícios do tratamento de dados, a ser preenchida pelas partes interessadas para esclarecer potenciais riscos operacionais e éticos.

Desta maneira, é possível utilizar este trabalho como fonte para a elaboração de futuros artefatos.

5.2 Trabalhos futuros

Em termos do projeto CICFriend dentro do contexto SmartUnB.ECOS diversos trabalhos já estão em andamento que dão continuidade na implementação de novas funcionalidades para a rede social, e na implementação de outros tipos de serviços para o ecossistema.

Para a implementação das funcionalidades de gamificação que está sendo desenvolvida, uma oportunidade de trabalho futuro com foco em ética é mensurar como a distribuição de *badges* é representativa da comunidade de usuários. Caso não seja, trabalho adicional pode entender quais formas de intervenção seriam possíveis para aumentar a representatividade, ou mesmo quais tipos de atividades podem estar sendo ignoradas em detrimento de outras que são específicas de um tipo de contexto sociocultural.

Abordando a problemática do consentimento informado, e com o intuito de fomentar a confiança, minimizar as assimetrias de poder inerentes do ambiente educacional, e prover controle sobre seus dados para alunos, uma oportunidade de trabalho futuro é a análise da viabilidade de implementar protocolos de modelo P3P [46] - The platform for privacy preferences (a plataforma para preferências de privacidade) - e sua usabilidade. O protocolo foi desenvolvido no início dos anos 2000 e especifica um formato padrão para políticas de privacidade de sites de forma que as tecnologias se comuniquem, avaliem e respeitem as escolhas de privacidade individuais definidas em aplicativos e ferramentas digitais. Os usuários definem suas preferências de privacidade em seus navegadores da web; o navegador, atuando como agente, interpreta as políticas de privacidade do site; e o navegador determina se o site respeita ou não as preferências de privacidade dos usuários e

quando os dois são incongruentes, o navegador avisa o usuário sobre a incompatibilidade de preferência de privacidade, bloqueia os cookies e solicita a entrada do usuário para saber como proceder.

Ainda na questão de consentimento, porém agora de um ponto de vista educacional, um dos principais lacunas identificados na literatura foi a falta de instrução, tanto para alunos quanto para professores e administradores, sobre os riscos do compartilhamento de dados pessoais e a importância de gerenciar dados estudantis de maneira responsável. Trabalhos futuros que colaborem para conscientização da importância de compreender melhor os riscos e benefícios envolvidos no compartilhamento de dados serão de grande valor para a construção de uma nova visão sobre o valor dos dados, que está crescendo cada dia mais na nossa sociedade.

Para alunos de cursos de computação, a necessidade de instrução vai um passo além das questões de compartilhamento de dados pessoais. Como abordado por Bispo Jr [24], há a necessidade de uma formação ética, pois é necessário abordar questões que fogem da binaridade em que sistemas operam pois muitas vezes os desafios éticos estão atrelados a uma causa temporal ou contextual. É necessário que os alunos e futuros profissionais de computação estejam preparados para analisar possíveis riscos éticos não-triviais, e para isso é preciso se basear na perspectiva do usuário, na interpretação de princípios éticos e na interação deles com o sistema sendo proposto. Estudos de como incorporar a ética no estudo da computação acrescentarão uma visão mais humana a computação, que com o advento da IA se vê cada vez mais necessária.

Referências

[1] Schwab, K. e D.M. Miranda: *A Quarta Revolução Industrial*. Edipro, 2019, ISBN 9788552100461. https://books.google.com.br/books?id=XZSWDwAAQBAJ. 1

[2] Lee, Kai Fu: *Inteligência artificial*. Globo Livros, 2019, ISBN 9786580775057. 1

[3] Istenič Starčič, Andreja: *Human learning and learning analytics in the age of artificial intelligence*. British Journal of Educational Technology, 50(6):2974–2976, 2019. https://bera-journals.onlinelibrary.wiley.com/doi/abs/10.1111/bjet.12879. 1

[4] Elias, Tanya: *Learning analytics*. Learning, páginas 1–22, 2011. 1

[5] Valente, Jonas: *Brasil tem 134 milhões de usuários de internet, aponta pesquisa*. Agência Brasil, 2020. https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa. 1

[6] Faizi, Rdouan, Abdellatif El Afia e Raddouane Chiheb: *Exploring the potential benefits of using social media in education*. International Journal of Engineering Pedagogy (iJEP), 3(4):50–53, 2013. 1

[7] Wood, Laura: *Artificial intelligence (ai) in education - global market trajectory and analytics*. Relatório Técnico, Global Industry Analysts, Inc, 2021. https://www.researchandmarkets.com/reports/5301849/artificial-intelligence-ai-in-education. 1

[8] Lawson, Celeste, Colin Beer, Dolene Rossi, Teresa Moore e Julie Fleming: *Identification of 'at risk'students using learning analytics: the ethical dilemmas of intervention strategies in a higher education institution*. Educational Technology Research and Development, 64(5):957–968, 2016. 1, 12, 27, 29, 30

[9] Brasil: *Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais (lgpd)*. Diário Oficial da República Federativa do Brasil, 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. 2, 20, 35

[10] Nóbrega, Germana e Fernando Cruz: *Rumo a um ecossistema educacional apoiado por computador e socialização em rede descentralizada*. Em *Anais Estendidos do XVII Simpósio Brasileiro de Sistemas Colaborativos (SBSC 2021)*, páginas 36–41, Porto Alegre, RS, Brasil, 2021. SBC. https://sol.sbc.org.br/index.php/sbsc_estendido/article/view/16033. 2, 17

[11] European Commission: *Ethics Guidelines for Trustworthy AI High-Level Expert Group on artificial intelligence*, abril 2019. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai, acesso em 2020-10-08. 5

[12] Kurzweil, Ray: *How to create a mind: The secret of human thought revealed*. Penguin, 2013. 5

[13] Sartor, Giovanni e Francesca Lagiola: *The impact of the general data protection regulation (gdpr) on artificial intelligence*. Relatório Técnico, Panel for the Future of Science and Technology, Brussels, 2020, ISBN 978-92-846-6771-0. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf. 6

[14] European Commission: *White paper on artificial intelligence: a european approach to excellence and trust*. White paper COM(2020) 65 final, European Commission, Brussels, fevereiro 2020. https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en. 7

[15] Kang, Cecilia e Sheera Frenkel: *Facebook says cambridge analytica harvested data of up to 87 million users*. The New York Times, 2018. https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html. 7

[16] Anderson, Berit e Brett Horvath: *The rise of the weaponized ai propaganda machine*. Medium, 2017. https://medium.com/join-scout/the-rise-of-the-weaponized-ai-propaganda-machine-86dac61668b. 7

[17] Hern, Alex: *How to check whether facebook shared your data with cambridge analytica*. The Guardian, 2018. https://www.theguardian.com/technology/2018/apr/10/facebook-notify-users-data-harvested-cambridge-analytica. 7

[18] Lewis, Paul e Paul Hilder: *Leaked: Cambridge analytica's blueprint for trump victory*. The Guardian, 2018. https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory. 7

[19] Holmes, Wayne, Maya Bialik e Charles Fadel: *Artificial intelligence in education*. Boston: Center for Curriculum Redesign, 2019. 8, 9, 29

[20] Holmes, Wayne, Kaska Porayska-Pomsta, Ken Holstein, Emma Sutherland, Toby Baker, Simon Buckingham Shum, Olga C Santos, Mercedes T Rodrigo, Mutlu Cukurova, Ig Ibert Bittencourt e Kenneth R Koedinger: *Ethics of AI in education: towards a community-wide framework*. International Journal of Artificial Intelligence in Education, páginas 1–23, 2021. 9, 10, 14, 29, 30

[21] Brasil: *Resolução nº 196, de 10 d outubro de 1996*. Diário Oficial da República Federativa do Brasil, 1996. https://bvsms.saude.gov.br/bvs/saudelegis/cns/1996/res0196_10_10_1996.html. 11

[22] Brasil: *Resolução nº 466, de 12 de dezembro de 2012*. Diário Oficial da República Federativa do Brasil, 2012. https://bvsms.saude.gov.br/bvs/saudelegis/cns/2012/res0466_12_12_2012.html. 11

[23] Brasil: *Resolução nº 510, de 7 de abril de 2016*. Diário Oficial da República Federativa do Brasil, 2016. https://bvsms.saude.gov.br/bvs/saudelegis/cns/2016/res0510_07_04_2016.html. 11, 41

[24] Bispo Jr., Esdras, Liliane Fonseca e Simone Santos: *Reflexões e desafios sobre a formação na Ética em pesquisa na computação envolvendo humanos*. Em *Anais do XXIX Workshop sobre Educação em Computação*, páginas 488–497, Porto Alegre, RS, Brasil, 2021. SBC. https://sol.sbc.org.br/index.php/wei/article/view/15940. 11, 46

[25] Fronza, Cátia de Azevedo: *Submissão de projeto de pesquisa ao Comitê de Ética: da Plataforma Brasil ao Parecer Consubstanciado*, capítulo 7. SBC, 2020. (Série Metodologia de Pesquisa em Informática na Educação, v. 1), 2020. 11

[26] Slade, Sharon e Paul Prinsloo: *Learning analytics: Ethical issues and dilemmas*. American Behavioral Scientist, 57(10):1510–1529, 2013. 12, 27, 28, 29, 30, 32

[27] Pardo, Abelardo e George Siemens: *Ethical and privacy principles for learning analytics*. British Journal of Educational Technology, 45(3):438–450, 2014. 12, 27, 28

[28] Prinsloo, Paul e Sharon Slade: *Ethics and Learning Analytics: Charting the (Un)Charted*, páginas 49–57. SoLAR, março 2017, ISBN 978-0-9952408-0-3. 12

[29] Slade, Sharon e Alan Tait: *Global guidelines: Ethics in learning analytics*. International Council for Open and Distance Education, 2019. 13, 27, 28, 29, 30, 32

[30] Kitto, Kirsty e Simon Knight: *Practical ethics for building learning analytics*. British Journal of Educational Technology, 50(6):2855–2870, 2019. 13, 29

[31] Ferguson, Rebecca: *Ethical challenges for learning analytics*. Journal of Learning Analytics, 6(3):25–30, 2019. 13, 27, 28, 29, 30

[32] Selwyn, Neil: *What's the problem with learning analytics?* Journal of Learning Analytics, 6(3):11–19, 2019. 13

[33] Holmes, Wayne, Duygu Bektik, Beverly Woolf e Rose Luckin: *Ethics in aied: Who cares?* 20th International Conference on Artificial Intelligence in Education (AIED'19), 2019. 13

[34] Vincent-Lancrin, Stéphan e Reyer van der Vlies: *Trustworthy artificial intelligence (ai) in education*. OECD Education Working Papers, 2020. https://www.oecd-ilibrary.org/content/paper/a6c90fa9-en. 13, 27, 28

[35] Beardsley, Marc, Judit Martínez-Moreno, Patricia Santos e Davinia Hernández-Leo: *Supporting students in making informed data sharing decisions: from comprehension to consenting*. Em *2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)*, páginas 175–179, 2020. 14, 24, 25, 29

[36] Pargman, Teresa Cerratto e Cormac McGrath: *Mapping the terrain of ethics in learning analytics: A systematic literature review of empirical research.* Journal of Learning Analytics, 2021. 14, 27, 28, 29, 30

[37] Scott, John: *Social network analysis.* Sociology, 22(1):109–127, 1988. https://doi.org/10.1177/0038038588022001007. 16

[38] Jéssica Oliveira, Germana Nóbrega, Fernando Cruz e Roberta Oliveira: *Decentralized social network for the campus: historical claims meet contemporary needs.* Em *Anais da XVI Conferência Latino-americana de Tecnologias de Aprendizagem (LACLO 2021)*. LACLO, 2021. 16

[39] Oliveira, Jéssica: *Rede social descentralizada em contexto acadêmico: Caracterização e potencialidades*, 2021. Monografia (Graduação em Engenharia de Computação). 16

[40] De Salve, Andrea, Paolo Mori e Laura Ricci: *A survey on privacy in decentralized online social networks.* Computer Science Review, 27:154–176, 2018, ISSN 1574-0137. https://www.sciencedirect.com/science/article/pii/S1574013717301557. 17, 18

[41] Carvalho, Luiz Paulo, Jonice Oliveira e Claudia Cappelli: *Pesquisas em análise de redes sociais e lgpd, análises e recomendações.* Em *Anais do IX Brazilian Workshop on Social Network Analysis and Mining*, páginas 73–84. SBC, 2020. 20

[42] Batista, Luana Scandian e Marcelo Fernando Quiroga Obregón: *Os impactos do regulamento europeu geral sobre proteção de dados (eu gdpr) no brasil (the impacts of the general data protection regulation (eu gdpr) in brazil los impactos del reglamento europeo general de protección de.* Derecho y Cambio Social, 2020. 20

[43] Carvalho, Thaís Abreu: *Aplicabilidade da lei geral de proteção de dados e da metodologia "privacy by design" nos termos de uso e de política de privacidade.* Faculdade de Direito de Vitória, 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito). 23

[44] Westin, Alan F: *Privacy and freedom.* Washington and Lee Law Review, 25(1):166, 1968. 24

[45] Solove, Daniel J: *Understanding privacy.* Harvard University Press, May, 2008. 24

[46] Jones, Kyle ML: *Learning analytics and higher education: a proposed model for establishing informed consent mechanisms to promote student privacy and autonomy.* International Journal of Educational Technology in Higher Education, 16(1):1–22, 2019. 24, 45

[47] Masur, Philipp K.: *Theories of Privacy*, páginas 33–68. Springer International Publishing, Cham, 2019. https://doi.org/10.1007/978-3-319-78884-5_3. 24

[48] Beardsley, Marc, Judit Martínez Moreno, Milica Vujovic, Patricia Santos e Davinia Hernández-Leo: *Enhancing consent forms to support participant decision making in multimodal learning data research.* British Journal of Educational Technology, 51(5):1631–1652, 2020. 25, 26

[49] Nishimura, Adam, Jantey Carey, Patricia J Erwin, Jon C Tilburt, M Hassan Murad e Jennifer B McCormick: *Improving understanding in the research informed consent process: a systematic review of 54 interventions tested in randomized control trials.* BMC medical ethics, 14(1):1–15, 2013. 25

[50] Jefford, M. e R. Moore: *Improvement of informed consent and the quality of consent documents.* The Lancet Oncology, 9(5):485–493, 2008. 26

[51] Young, D.R., D.T. Hooker e F.E. Freeberg: *Informed consent documents: Increasing comprehension by reducing reading level.* IRB, 12(3):1–5, 1990. 26

[52] Villafranca, A., S. Kereliuk, C. Hamlin, A. Johnson e E. Jacobsohn: *The appropriateness of language found in research consent form templates: A computational linguistic analysis.* PLoS One, 12(2):0169143, 2017. 26

[53] Perrault, E.K. e D.M. Keating: *Seeking ways to inform the uninformed: Improving the informed consent process in online social science research.* Journal of empirical research on human research ethics : JERHRE, 13(1):50–60, 2018. `https://doi.org/10.1177/1556264617738846`. 26

[54] Bjørn, E., P. Rossel e S. Holm: *Can the written information to research subjects be improved?–an empirical study.* Journal of Medical Ethics, 25(3):263–267, 1999. 26

[55] Wittenberg, K.M. e H.B. Dickler: *Universal use of short and readable informed consent documents: How do we get there? creating informed consent documents that inform: A literature review.* Association of American Medical Colleges Appendix C, 2007. 26

[56] Hallinan, Z.P., A. Forrest, G. Uhlenbrauck, S. Young e R. McKinney, Jr: *Barriers to change in the informed consent process: A systematic literature.* IRB, 38(3):1–10, 2016. 26

[57] Kadam, R.A.: *Informed consent process: A step further towards making it meaningful!* Perspectives in Clinical Research, 8(3):107–112, 2017. 26

[58] Lorenzen, B., C.E. Melby e B. Earles: *Using principles of health literacy to enhance the informed consent process.* AORN Journal, 88(1):23–29, 2008. 26

[59] Manta, C.J., J. Ortiz, B.W. Moulton e S.S. Sonnad: *From the patient perspective, consent forms fall short of providing information to guide decision making.* Journal of Patient Safety, página 00000 000310, 2016. `http://dx.doi.org/10.1097/pts.00000`. 26

[60] Kass, N.E., H.A. Taylor, J. Ali, K. Hallez e L. Chaisson: *A pilot study of simple interventions to improve informed consent in clinical research: Feasibility, approach, and results.* Clinical Trials, 12(1):54–66, 2015. 26

[61] Tait, A.R., T. Voepel-Lewis, A. Robinson e S. Malviya: *Priorities for disclosure of the elements of informed consent for research: A comparison between parents and investigators.* Pediatric Anesthesia, 12(4):332–336, 2002. 26

[62] Dranseika, V., J. Piasecki e M. Waligora: *Relevant information and informed consent in research: In defense of the subjective standard of disclosure.* Science and Engineering Ethics, 23(1):215–225, 2017. 26

[63] Karbwang, J., N. Koonrungsesomboon, C.E. Torres, E.B. Jimenez, G. Kaur, R. Mathur e M.A. Malek: *What information and the extent of information research participants need in informed consent forms: A multi-country survey.* BMC Medical Ethics, 19(1):79, 2018. 26

[64] Knepp, Michael M.: *Using questions to improve informed consent form reading behavior in students.* Ethics and Behavior, 28(7):560–577, 2018. 26

[65] Siemens, George e Phil Long: *Penetrating the fog: Analytics in learning and education.* EDUCAUSE review, 46(5):30, 2011. 27

[66] Ferguson, Rebecca, Tore Hoel, Maren Scheffel e Hendrik Drachsler: *Guest editorial: Ethics and privacy in learning analytics.* Journal of learning analytics, 3(1):5–15, 2016. 27, 28, 29

[67] Economia, Ministério da: *Guia de elaboração de termo de uso e política de privacidade para serviços públicos.* `https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_tupp.pdf`, 2021. 34, 35

[68] Freitas, Carlas: *Como elaborar uma política de privacidade aderente à lgpd?* SERPRO Notícias, 2019. 36

[69] Brasil: *Lei nº 9.394, de 20 de dezembro de 1996. lei de diretrizes e bases da educação nacional.* Diário Oficial da República Federativa do Brasil, 2018. `https://www2.senado.leg.br/bdsf/bitstream/handle/id/70320/65.pdf`. 37

[70] Martins, Stefan e Lucia Filgueiras: *Métodos de avaliação de apreensibilidade das informações textuais: uma aplicação em sítios de governo eletrônico.* Em *proceeding of Latin American Conference on Human-Computer Interaction (CLIHC 2007). Rio de Janeiro, Brazil*, 2007. 37

[71] Economia, Ministério da: *Guia de boas práticas lgpd.* `https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf`, 2020. 38

Apêndice A

Termo de Uso, Política de Privacidade e Declaração de Privacidade CICFriend

A.1 Declaração de Privacidade

- O que é o CICFriend?

Uma rede social! Aqui você pode postar dúvidas, divulgar projetos, mandar mensagens, participar de fóruns das suas disciplinas e muito mais.

- E a minha privacidade?

O CICFriend é uma iniciativa do Departamento de Ciência da Computação da UnB e sua inscrição é feita pelo e-mail da UnB. Só vamos usá-lo para mandar notificações. O seu nome aparece para todos na sua página de perfil.

- E os meus dados?

Seus dados são seus! Você pode exportá-los e excluir seu perfil quando quiser. Você escolhe quem pode e não pode ver cada uma das suas publicações. Não vamos fazer nada com seus dados sem antes pedir seu consentimento!

- E o que não pode fazer?

Não pode nenhum tipo de assédio, discurso de ódio, violência ou *bullying*! Caso algum conteúdo desobedeça as regras da universidade, ou seja ilegal de qualquer maneira, medidas administrativas e legais podem ser tomadas. Se encontrar algum conteúdo malicioso, denuncie para o administrador.

Para mais informações e dados de contato, ver Termo de Uso e Politica de Privacidade.

Ao clicar em Cadastre-se, você concorda com nossos Termos de Uso e Política de Dados.

A.2 Termo de Uso

Quais informações estão presentes neste documento?

Neste Termo de Uso, o usuário do serviço CICFriend encontrará informações sobre:

1. Termos e Políticas aplicáveis;
2. Definições dos termos utilizados;
3. Quais são as leis e normativos aplicáveis a esse serviço?
4. Descrição do serviço;
5. Direitos dos usuários;
6. Responsabilidades dos usuários;
7. Responsabilidade do operador com meu dados;
8. Informações para contato.

Para informações sobre o tratamento de dados, ver nossa Política de Privacidade

1. **Aceitação do Termo de Uso e Política de Privacidade**

Ao utilizar os serviços, o usuário confirma que leu e compreendeu o Termo de uso e a Política de Privacidade do CIC Friends e concorda em ficar vinculado a eles.

2. **Definições**

Para melhor compreensão deste documento, tanto neste Termo de Uso quanto na Política de Privacidade, consideram-se:

Agentes de tratamento: o controlador e o operador.

Consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Órgão de pesquisa: Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Usuários (ou "Usuário", quando individualmente considerado): todas as pessoas naturais que utilizarem o serviço CICFriend.

3. **Quais são as leis e normativos aplicáveis a esse serviço?**

-Lei nº 13.709, de 14 de agosto de 2018: Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

4. **Descrição do serviço**

O que é o CICFriend?

O CICFriend é uma rede social baseada no software Friendica. Através dela você pode se conectar a outros alunos, professores e técnicos administrativos que também se inscreveram.

Nela é possível postar dúvidas, divulgar projetos, mandar mensagens, participar de fóruns de disciplinas ou de interesses em comum, agendar reuniões e muito mais.

Essa é uma iniciativa do Departamento de Ciência da Computação da Universidade de Brasília. Essa rede social é descentralizada, o que significa você tem mais controle sobre seus dados, sobre quem pode ver suas publicações e sobre qual provedor de serviço você vai escolher para hospedar seus dados.

É possível acessar o CICFriend através de um navegador de Internet ou através de um aplicativo de dispositivo móvel.

5. **Quais são os direitos do usuário do serviço?**

O usuário do serviço possui os seguintes direitos, conferidos pela Lei de Proteção de Dados Pessoais e nativos da plataforma Friendica:

Direito de confirmação e acesso (Art. 18, I e II): é o direito do usuário de obter do serviço a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais. Somente usuários cadastrados serão objeto de tratamento.

Direito de retificação (Art. 18, III): é o direito de solicitar a correção de dados incompletos, inexatos ou desatualizados. É possível realizar a retificação através da edição do seu perfil ou através das configurações.

Direito à limitação do tratamento dos dados (Art. 18, IV): é o direito do usuário de limitar o tratamento de seus dados pessoais, podendo exigir a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados. Somente os dados essenciais ao funcionamento do CICFriend serão tratados, ou seja, dados para que haja a comunicação segura entre os usuários. Qualquer adição de serviços será informada e seu consentimento será pedido.

Direito de oposição (Art. 18, § 2º): é o direito do usuário de, a qualquer momento, se opor ao tratamento de dados por motivos relacionados com a sua situação particular, com fundamento em uma das hipóteses de dispensa de consentimento ou em caso de descumprimento ao disposto na Lei Geral de Proteção de Dados. Caso se oponha ao tratamento de dados, você pode solicitar a exportação dos seus dados e a exclusão da sua conta.

Direito de portabilidade dos dados (Art. 18, V): é o direito do usuário de realizar a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial. O usuário pode, a qualquer momento, realizar a exportação dos seus dados e está livre para escolher outro provedor de serviço.

Direito de não ser submetido a decisões automatizadas (Art. 20, LGPD): o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. Qualquer implementação de decisões automatizadas serão informadas e o consentimento será pedido.

6. **Quais são as obrigações dos usuários que utilizam o serviço?**

O usuário se responsabiliza pela precisão e veracidade dos dados informados e reconhece que a inconsistência destes poderá implicar a impossibilidade de se utilizar o serviço CICFriend.

Durante a utilização do serviço, a fim de resguardar e de proteger os direitos de terceiros, o usuário se compromete a fornecer somente seus dados pessoais, e não os de terceiros.

O login e senha só poderão ser utilizados pelo usuário cadastrado. Ele se compromete em manter o sigilo da senha, que é pessoal e intransferível, não sendo possível, em qualquer hipótese, a alegação de uso indevido, após o ato de compartilhamento.

O usuário do serviço é responsável pela atualização das suas informações pessoais e consequências na omissão ou erros nas informações pessoais cadastradas.

A responsabilidade pelo conteúdo criado pelos usuários - postagens, mensagens e muito mais - é do usuário. O operador não é de forma alguma responsável.

Os usuários são encorajados a se comunicar de forma respeitosa. Em particular, mas não exclusivamente, assédio, discurso de ódio, racismo, violência e bullying não são tolerados.

Solicita-se aos usuários que não publiquem qualquer conteúdo que viole a lei aplicável na República Federativa do Brasil ou as normas vigentes da Universidade de Brasília. Caso o conteúdo viole as leis ou normas e o operador for informado, este entrará em contato com o usuário, também publicamente, e pedirá esclarecimentos sobre o problema e, se necessário, a exclusão do conteúdo.

Se não houver outra opção, o operador excluirá o conteúdo.

Além da remoção de contribuições civil ou criminalmente relevantes, a operadora reserva-se o direito de remover conteúdo que esteja à beira da legalidade. Essa definição inclui, mas não se limita a, conteúdos de representações pornográficas ou eróticas de menores.

O provedor não poderá ser responsabilizado pelos seguintes fatos:

a. Equipamento infectado ou invadido por atacantes;

b. Equipamento avariado no momento do consumo de serviços;

c. Proteção do computador;

d. Proteção das informações baseadas nos computadores dos usuários;

e. Abuso de uso dos computadores dos usuários;

f. Monitoração clandestina do computador dos usuários;

g. Vulnerabilidades ou instabilidades existentes nos sistemas dos usuários;

h. Perímetro inseguro;

Este serviço é provido através de um software de código aberto e gratuito, sem fins comerciais.

Ao acessar o aplicativo, os usuários declaram que irão respeitar todos os direitos de propriedade intelectual e os decorrentes da proteção de marcas, patentes e/ou desenhos industriais, depositados ou registrados em, bem como todos os direitos referentes a terceiros que porventura estejam, ou estiverem de alguma forma, disponíveis no serviço.

É vedada a utilização do serviço para finalidades comerciais, publicitárias ou qualquer outra que contrarie a finalidade para a qual foi concebido, conforme definido neste documento.

Os visitantes e usuários assumem toda e qualquer responsabilidade, de caráter civil e/ou criminal, pela utilização indevida das informações, textos, gráficos, marcas, imagens, enfim, todo e qualquer direito de propriedade intelectual ou industrial do serviço.

Em nenhuma hipótese, o provedor de serviço será responsável pela instalação no equipamento do Usuário ou de terceiros, de códigos maliciosos (vírus, trojans, malware, worm, bot, backdoor, spyware, rootkit, ou de quaisquer outros que venham a ser criados), em decorrência da navegação na Internet pelo Usuário.

Tendo em vista que o serviço lida com informações pessoais, o usuário concorda que não usará robôs, sistemas de varredura e armazenamento de dados (como “spiders” ou “scrapers”), links escondidos ou qualquer outro recurso escuso, ferramenta, programa, algoritmo ou método coletor/extrator de dados automático para acessar, adquirir, copiar ou monitorar o serviço, sem permissão expressa por escrito do órgão.

7. **Quais são as responsabilidades do operador com meus dados?**

O provedor de serviço, no papel de custodiante das informações pessoais dos usuários, deve cumprir todas as legislações inerentes ao uso correto dos dados pessoais do cidadão de forma a preservar a privacidade dos dados utilizados na plataforma.

Atualizações e alterações a este Termo de Uso serão informadas através de notificações e publicadas por meio do sítio (à ser inserido). Novo consentimento será requerido.

Em hipótese alguma, o serviço e seus colaboradores responsabilizam-se por eventuais danos diretos, indiretos, emergentes, especiais, imprevistos ou multas causadas, em qualquer matéria de responsabilidade, seja contratual, objetiva ou civil (inclusive negli-

gência ou outras), decorrentes de qualquer forma de uso do serviço, mesmo que advertida a possibilidade de tais danos.

Caso o usuário descumpra o Termo de Uso ou a Política de Privacidade, ele poderá ser investigado em razão de má conduta, o provedor de serviço poderá restringir seu acesso. O usuário também poderá responder legalmente por essa conduta.

O provedor de serviço poderá, quanto às ordens judiciais de pedido de informações, compartilhar informações necessárias para investigações ou tomar medidas relacionadas a atividades ilegais, suspeitas de fraude ou ameaças potenciais contra pessoas, bens ou sistemas que sustentam o serviço ou de outra forma necessária para cumprir com as obrigações legais. Caso ocorra, o operador notificará os titulares dos dados, salvo quando o processo estiver em segredo de justiça.

O provedor de serviço faz todos os esforços para operar a plataforma o mais ininterruptamente e livre de perdas possível. No entanto, nenhuma responsabilidade é assumida por isso. Em caso de perda de dados, a operadora informará os usuários.

Para obter uma operação segura e sem problemas, os registros de servidor (arquivos de log) são criados automaticamente. Estes são tipicamente excluídos após três, mas no máximo após sete dias. Além disso, a operadora cria regularmente backups de dados dos aplicativos, arquivos e do banco de dados, a fim de proteger os usuários contra a perda de dados. Estes são normalmente excluídos após sete dias, mas no máximo após um mês.

8. **Qual o contato pelo qual o usuário do serviço pode tirar suas dúvidas?**

Caso o usuário tenha alguma dúvida sobre este Termo de Uso, ele poderá entrar em contato com o time de suporte através do email suporte@cicfriend.cic.unb.br, ou com a responsável pelo e-mail gmnobrega@unb.br.

A.3 Política de Privacidade

Nesta Política de Privacidade o usuário do serviço CICFriend encontrará informações sobre:

1. Quem são os responsáveis pelo tratamento dos dados;
2. Tudo sobre o tratamento dos meus dados;
3. Compartilhamento de dados;
4. Segurança dos dados;
5. Cookies;

6. Tratamento posterior para outras finalidades;

Esta Política de Privacidade foi elaborada em conformidade com a Lei Federal n. 12.965 de 23 de abril de 2014 (Marco Civil da Internet) e com a Lei Federal n. 13.709, de 14 de agosto de 2018 (Lei de Proteção de Dados Pessoais).

Esta Política de Privacidade poderá ser modificada, a qualquer momento, devido a atualização normativa, ou para adaptá-las às evoluções do serviço CICFriend, seja pela disponibilização de novas funcionalidades, seja pela supressão ou modificação daquelas já existentes. Convidamos os usuários a consultar periodicamente esta seção.

O usuário também será explicitamente notificado em caso de alteração dessa Política de Privacidade.

O site se compromete a cumprir as normas previstas na Lei Geral de Proteção de Dados (LGPD), e respeitar os princípios dispostos no Art. 6º:

(i) - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

(ii) - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

(iii) - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

(iv) - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

(v) - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

(vi) - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

(vii) - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

(viii) - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

(ix) - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

(x) - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

1. Quem é o responsável pelo tratamento de dados?

   Este é um projeto do Departamento de Ciência da Computação da Universidade de Brasília.

   Responsável pelas decisões referentes ao tratamento de dados pessoais (controladora):

   Professora responsável: Germana Menezes da Nóbrega.

   Endereço: Prédio de Ciência da Computação e Estatística - CIC/EST, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Asa Norte, Brasília, DF.

   E-mail: gmnobrega@unb.br.

   Telefone: +55 61 3107-2226.

   Realiza o tratamento de dados pessoais (Operador):

   A definir.

2. Tudo sobre o tratamento dos meus dados

   O CICFriend é uma rede social, e, para conectar você aos outros usuários, atualizar o seu *feed* e sugerir publicações, nós precisamos tratar seu dados. Segue os dados que serão tratados:

   Seus dados de inscrição: -Nome completo; -Nome social; -Endereço de e-mail; -Endereço (se informado); -Número de telefone (se informado).

   Suas publicações: - Entradas de texto; - Fotografias; - Vídeos.

   Dados de uso: - Sites visitados; - Interesse em conteúdos; - Tempos de acesso.

   Metadados e dados de comunicação: - Informações do dispositivo; - Endereços IP.

   Finalidade de processamento: - Provisão da oferta online, suas funções e conteúdo - Responder solicitações de contato e Comunicação com os usuários - Medidas de segurança

   Explicando um pouco melhor como funciona o tratamento de dados:

   Como usamos seus dados de inscrição: Para se cadastrar, as informações obrigatórias serão informadas e algumas opcionais. Os dados que você inserir serão

usados para que você possa utilizar nossa rede. Podemos entrar em contato via email sobre: informações do seu cadastro, alterações nos nossos serviços e eventual questão técnica.

Como usamos seus dados de publicações: Para o funcionamento da rede social precisamos tratar os dados das suas publicações, para que seja transmitida aos seus amigos ou de acordo com nível de acesso que escolher. Se quiser, é possível fazer integrações com outras redes sociais, caso opte por isso, seus dados serão compartilhados com terceiros, mais detalhes sobre na próxima seção

Se forem deixados comentários ou outras contribuições, seus endereços IP serão armazenados por 7 dias. Isso é feito para nossa segurança se alguém deixa conteúdo ilegal em comentários e contribuições (insultos, propaganda política proibida, etc.). Neste caso, nós mesmos podemos ser processados pelo comentário ou contribuição e, portanto, estamos interessados na identidade do autor.

Como usamos seus dados de uso: Para exibirmos conteúdos relevantes para você no seu feed, nós utilizamos os seus dados de uso, como principais sites internos visitados e seu interesse em conteúdos.

Como usamos os metadados e dados de comunicação: Nós coletamos também dados sobre cada acesso ao servidor no qual este serviço está hospedado (os chamados arquivos de log de servidor). Os dados de acesso incluem: o nome do site acessado, arquivo, data e hora de recuperação, quantidade de dados transferidos, notificação de recuperação bem-sucedida, tipo e versão do navegador, sistema operacional do usuário, URL de remetente (a página visitada anteriormente), endereço IP e o provedor solicitante.

As informações do arquivo de registro são armazenadas por razões de segurança (ex. para investigar o uso indevido ou fraude) por um máximo de 7 dias e depois excluídas. Os dados cujo novo armazenamento é necessário para fins probatórios são excluídos da exclusão até que o respectivo incidente seja finalmente esclarecido.

Como parte do uso de nossas funções de registro e login, bem como o uso da conta de usuário, armazenamos o endereço IP e o tempo da respectiva ação do usuário.

O armazenamento ocorre com base em nossos interesses legítimos, bem como na proteção do usuário contra uso indevido e outros usos não autorizados. Em princípio, esses dados não serão repassados a terceiros, a menos que seja necessário para fins legais. Os endereços IP são anonimizados ou excluídos após 7 dias, no máximo.

Ao excluir sua conta: Se os usuários tiverem encerrado sua conta de usuário, seus dados serão excluídos em relação à conta do usuário. É responsabilidade dos usuá-

rios fazer backup de seus dados antes do término do contrato em caso de rescisão. Temos o direito de excluir irremediavelmente todos os dados do usuário armazenados durante o prazo do contrato.

Ao entrar em contato com a gente: Ao entrar em contato conosco (via formulário de contato, e-mail, telefone ou via redes sociais), os seus dados de usuário são tratados para processar a solicitação de contato.

Excluímos os pedidos se eles não forem mais necessários. Revisamos a necessidade a cada dois anos.

3. Compartilhamento de dados

   Caso decida integrar outras redes sociais ao CICFriend, seja a outros nós Friendica ou a serviços externos como o Twitter, o operador não pode fazer nenhuma declaração. As normas de proteção de dados da respectiva plataforma devem ser observadas aqui.

   Seção a ser editada após decisão de AddOns que serão utilizados

   Para que seja possível a publicação de conteúdo de terceiros (vídeos, links, dentre outros) disponíveis online, é necessário o compartilhamento do endereço de IP do usuário, visto que sem o endereço IP o provedor terceiro não poderia enviar o conteúdo ao seu navegador.

   Nos esforçamos para usar apenas conteúdo cujos provedores usam apenas o endereço IP para a entrega do conteúdo ao usuário.

   - Vimeo: Podemos integrar os vídeos da plataforma "Vimeo"do provedor Vimeo Inc.: Departamento Jurídico, 555 West 18th Street Nova York, Nova York 10011, EUA.

     Política de Privacidade: `https://vimeo.com/privacy`.

     Gostaríamos de salientar que o Vimeo pode usar o Google Analytics e se referir à política de privacidade (`https://www.google.com/policies/privacy`),bem como opções de opt-out para o Google Analytics (`http://tools.google.com/dlpage/gaoptout?hl=de`) ou as configurações do Google para uso de dados para fins de marketing (`https://adssettings.google.com/`).

   - Youtube: Integramos os vídeos da plataforma "YouTube"do provedor Google LLC, 1600 Anfiteatro Parkway, Mountain View, CA 94043, EUA.

     Política de Privacidade: `https://www.google.com/policies/privacy/`, Opt-Out: `https://adssettings.google.com/authenticated`.

- OpenStreetMap: Integramos os mapas do serviço "OpenStreetMap"(`https://www.openstreetmap.de`), que são oferecidos com base na Licença aberta de banco de dados aberto (ODbL) pela OpenStreetMap Foundation (OSMF).

  Política de Privacidade: `https://wiki.openstreetmap.org/wiki/Privacy_Policy---`). Para nosso conhecimento, os dados dos usuários são usados pelo OpenStreetMap exclusivamente com o propósito de exibir as funções do mapa e cache das configurações selecionadas. Esses dados podem incluir, em particular, endereços IP e dados de localização dos usuários, que, no entanto, não são coletados sem o seu consentimento (geralmente realizados como parte das configurações de seus dispositivos móveis). Os dados podem ser processados nos EUA. Mais informações podem ser encontradas na política de privacidade do OpenStreetMap: `https://wiki.openstreetmap.org/wiki/Privacy_Policy`.

4. Segurança no tratamento dos dados pessoais do usuário

   O servico CICFriend se compromete a aplicar as medidas técnicas e organizativas aptas a proteger os dados pessoais de acessos não autorizados e de situações de destruição, perda, alteração, comunicação ou difusão de tais dados.

   Para a garantia da segurança, serão adotadas soluções que levem em consideração: as técnicas adequadas; os custos de aplicação; a natureza, o âmbito, o contexto e as finalidades do tratamento; e os riscos para os direitos e liberdades do usuário.

   O site utiliza criptografia para que os dados sejam transmitidos de forma segura e confidencial, de maneira que a transmissão dos dados entre o servidor e o usuário, e em retroalimentação, ocorra de maneira totalmente cifrada ou encriptada.

   No entanto, o site se exime de responsabilidade por culpa exclusiva de terceiro, como em caso de ataque de hackers ou crackers, ou culpa exclusiva do usuário, como no caso em que ele mesmo transfira seus dados a terceiro.

   O serviço CICFriend se compromete, ainda, a comunicar o usuário em prazo adequado caso ocorra algum tipo de violação da segurança de seus dados pessoais que possa lhe causar um alto risco para seus direitos e liberdades pessoais.

   A violação de dados pessoais é uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

   Por fim, o site se compromete a tratar os dados pessoais do usuário com confidencialidade, dentro dos limites legais.

5. Cookies

   Cookies são pequenos arquivos de texto enviados pelo site ao computador do usuário e que nele ficam armazenados, com informações relacionadas à navegação do site.

   Por meio dos cookies, pequenas quantidades de informação são armazenadas pelo navegador do usuário para que nosso servidor possa lê-las posteriormente. Podem ser armazenados, por exemplo, dados sobre o dispositivo utilizado pelo usuário, bem como seu local e horário de acesso ao site.

   É importante ressaltar que nem todo cookie contém dados pessoais do usuário, já que determinados tipos de cookies podem ser utilizados somente para que o serviço funcione corretamente.

   As informações eventualmente armazenadas em cookies também são consideradas dados pessoais e todas as regras previstas nesta Política de Privacidade também são aplicáveis a eles.

   Se o usuário não quiser que os cookies sejam armazenados em seu computador, ele será solicitado a desativar a opção correspondente nas configurações do sistema de seu navegador. Os cookies armazenados podem ser excluídos nas configurações do sistema do navegador. A exclusão de cookies pode levar a restrições funcionais desta oferta online.

   Para o serviço CICFriend informações anonimizadas podem ser armazenadas em cookies no dispositivo do usuário e contêm: informações técnicas sobre o navegador e sistema operacional; referências de sites; tempo de visita e outras informações sobre o uso de nossa oferta online, bem como ser combinadas com tais informações de outras fontes.

6. Tratamento posterior para outras finalidades;

   Dados anonimizados de acesso e uso poderão ser utilizados a fim de análise da utilização da rede e melhorias no sistema. Quaisquer outros tratamentos posteriores serão informados e o consentimento será requerido.

Apêndice B

Matriz de Riscos e Benefícios

Tipo tratamento	Riscos	Mitigações	Benefícios	Descrição	Perguntas Orientadoras
Coleta de dados	Risco da falta de informações sobre as finalidades do proessamento ou falta de engajamento com alunos levar ao não consentimento ou a um consentimento inválido. Risco do não engajamento com alunos levar a baixa utilização da solução.	Engajamento proativo com alunos para colaboração no uso e avaliação da solução.Transparência na apresentação da solução, dos tratamentos de dados realizados e seus fins. Integração com plataforma de diretório de acesso da universidade para autenticar dados de inscrição. Encriptação da comunicação via HTTPS.	Fornecimento do serviço online, cujos beneficios incluem: maior interação com professores e alunos, apoiar na concepção da rede social do CICFriend. Criação de perfil pessoal para interação com controle de acesso.	Avaliar riscos éticos e operacionais da etapa de coleta (operações de coleta, produção e recepção) de dados, especialmente os que tratam dos princípios de: transparência, consentimento informado e agência e responsabilidade do aluno.	Quais os riscos do fornecimento de dados inválidos? Quais os riscos da falta informações levar a um consentimento inválido? Quais os riscos do não engajamento com alunos? Quais os riscos de acesso não autorizado? Quais os riscos da coleção excessiva de dados?
Retenção	Risco da falta de informações sobre as finalidades do proessamento ou falta de engajamento com alunos levar ao não consentimento ou a um consentimento inválido. Risco do não	Controle de acesso lógico, backup de dados do servidor e comunicação clara sobre dados armazenados e seus períodos de retenção.	Fornecimento do serviço online. Criação de uma linha de tempo em forma de publicações.	Avaliar riscos éticos e operacionais na retenção (arquivamento e armazenamento) de dados, especialmente os que tratam dos princípios de: transparência, propriedade e controle de dados e acessibilidade.	Quais os riscos de acesso não autorizado? Quais os riscos de perda de dados? Quais os riscos inerentes do procedimentos para cumprir os prazos de retenção de dados? Quais os dados passíveis de anonimização? Quais dados podem ter tratamentos posteriores? Todos essas possibilidades foram informadas?
Processamento	Risco de enviesamento nas análises levar a bonificação indevida ou a falta dela, risco de extrapolação errônea de dados, risco de falta de consentimento a todo tipo de processamento.	Transparência quanto aos processamentos que serão realizados sobre os dados. Classificação de dados sensíveis e governança de dados.	Fornecimento do serviço online. Possibilidade de receber badges e recompensas por colaborações.	Avaliar riscos éticos e operacionais do processamento de dados, especialmente os que tratam dos princípios de: transparência, propriedade e controle de dados, validade e confiabilidade dos dados, responsabilidade institucional e obrigação de agir, valores culturais, inclusão e consentimento	Quais os riscos de uma classificação/agrupamento enviesado? Quais os riscos de processamento de dados sensíveis? Quais os riscos de reuso não informado? Quais os riscos de tratar os dados mais que o comunicado (transparência)? Quais os riscos de não agir sobre informação? Quais os riscos da extrapolação de dados? Quais os riscos de viés? Quais os riscos da avaliação levar à exclusão? Quais os riscos de modificação não autorizada? Quais os riscos de falha ou erro de processamento?
Compartilhamento	Risco de acesso indevido e riscos de interpretação errada de análises.	Controle de acesso à publicações por listas de acesso, inerentes do Friendica. Procedimentos para comunicação de análises bem definidos.	Fornecimento do serviço online. Rede de amigos podem visualizar e interagir com suas publicações.	Avaliar riscos éticos e operacionais do compartilhamento de dados, especialmente os que tratam dos princípios de: transparência, propriedade e controle de dados e acessibilidade, validade e confiabilidade dos dados, comunicações e consentimento	Quais os riscos de acesso indevido? Quais os riscos de compartilhamento de análises que são estatísticas? Quais os riscos de comunicação indevida como resultado de análises? Quais os riscos de compartilhamento além do consentido?
Eliminação	Risco de perda de dados, risco de reidentificação de dados com tecnologia mais avançada.	Processo de governança de dados bem estabelecido. Anonimização realizada visando a desidentificação completa do aluno.	Possibilidade de eliminação e portabilidade do perfil.	Avaliar riscos éticos e operacionais da eliminação de dados, especialmente os que tratam dos princípios de: transparência, propriedade e controle de dados e consentimento.	Quais os riscos na eliminação indevida de dados? Quais os riscos de perda de dados? Quais os riscos na anonimização de dados antes da eliminação para fins de reuso? Quais os risco de reidentificação de dados anonimizados? Quais os riscos sobre o direito de saber do tratamento de dados ocorrido?

Apêndice C

Termo de Consentimento Livre e Esclarecido CICFriend

Você está sendo convidado a participar da pesquisa "Avaliação da percepção do usuário da rede social CICFriend no contexto acadêmico".

Pesquisador: (inserir os nomes do pesquisador)

Graduando em (inserir curso), pela Universidade de Brasília, orientado pela professora Germana Menezes da Nóbrega

Objetivo da pesquisa - Identificar:

1. as expectativas para o uso de uma rede social no contexto da educação;
2. as vantagens e desvantagens no uso da rede;
3. possíveis melhorias a serem feitas.

Gostaria de saber se você gostaria de participar desta pesquisa.

Como será feita a pesquisa? A pesquisa será dividida em 3 momentos, antes, durante e após o uso da rede CICFriend:

Primeiro momento, antes do uso: Você vai responder um questionário sobre seu uso atual de redes sociais, suas expectativas para uma rede social na educação e se teria alguma funcionalidade que gostaria que existisse.

Segundo momento, durante o uso: Serão coletados dados de utilização da rede nos nossos servidores. Esses dados serão anonimizados e utilizados só para ver como foi utilizada a rede, quantos acessos foram registrados, quais conteúdos mais visitados etc. Serão 3 semanas de avaliação da rede.

Terceiro momento, após o uso: Será realizado um grupo focal através de uma reunião via videoconferência em que será discutido as percepções sobre o uso da rede, se supriu as expectativas mencionadas no questionário, e sugestões de melhorias.

A videoconferência será gravada para que não seja necessária a interrupção de ninguém para realizar anotações. A gravação será apagada após a extração das informações, que será feita anonimizando os participantes.

Podemos garantir que:

- Não serão divulgados nomes ou informações que possam te identificar;
- Seus dados só serão usados para este estudo;
- Sua participação é voluntária, e você pode desistir do estudo a qualquer momento, sem nenhum prejuízo a você;
- Se tiver dúvidas em relação à pesquisa, você pode entrar em contato comigo através do telefone 00000000 ou pelo e-mail email@email.com;
- Os resultados da pesquisa serão devolvidos através de uma apresentação realizada nas turmas participantes e serão publicados na comunidade científica através do meu Trabalho de Conclusão de Curso.
- A pesquisa apresenta risco mínimo que está relacionado ao risco no vazamento de dados pessoais, risco mitigado pelo processo de governança de dados em prática;
- Com esta pesquisa esperamos implantar a rede social CICFriend e aumentar a colaboração e interação entre alunos, professores e a administração da UnB.

Este projeto foi revisado e aprovado pelo Comitê de Ética em Pesquisa em Ciências Humanas e Sociais (CEP/CHS) da Universidade de Brasília. As informações com relação à assinatura do TCLE ou aos direitos do participante da pesquisa podem ser obtidas por meio do e-mail do CEP/CHS: `cep_chs@unb.br` ou pelo telefone: (61) 3107 1592.

(Para TCLE impresso) Este documento foi elaborado em duas vias, uma ficará com o pesquisador responsável pela pesquisa e a outra com você.

(Para TCLE digital) O seu aceite se dá pela devolução deste documento com sua assinatura digital.