**SEGURANÇA NA ERA DIGITAL: DESAFIOS LEGAIS E SOLUÇÕES**

Ana Esther Martins de Araújo

Danilo Marques Chamiço Caetano

Eduardo Camargo Bezerra

Jefferson Lucas R. Silva

João Teodoro da Silva Filho

Laryssa Santos Gomes

Victoria Freitas Ticly

Uni Processus

Brasília

2023

Resumo

O tema deste artigo é “Segurança na Era Digital: Desafios Legais e Soluções”. O presente projeto buscará evidenciar quais os impactos e implicações legais do uso da tecnologia no ensino, incluindo questões de privacidade, segurança de dados, direitos autorais e responsabilidade civil. O objetivo geral é “Realizar uma análise das implicações legais do uso de tecnologias digitais na educação, com foco em questões de privacidade, segurança de dados, direitos autorais e responsabilidade civil. ”. Os objetivos específicos são: “Identificar as principais questões legais relacionadas ao uso de tecnologias digitais na educação”; “Analisar as leis e normas existentes que regulam o uso de tecnologias digitais”; “Identificar as melhores práticas para garantir a privacidade e segurança dos dados dos alunos”; “Analisar os impactos dos direitos autorais no uso de materiais digitais na educação”; e “Identificar as responsabilidades legais dos envolvidos no processo educacional”.

Palavras-chave: Segurança Digital, Legislação e Tecnologia, Privacidade de Dados.

# Introdução

# Este trabalho escrito discute as implicações legais do uso de tecnologias digitais na educação, com foco em questões de privacidade, segurança de dados, direitos autorais e responsabilidade civil. O uso crescente de tecnologias digitais no ensino traz consigo diversas questões que precisam ser consideradas, como a proteção dos dados dos alunos, a garantia da privacidade no ambiente virtual, a autoria de conteúdos produzidos e compartilhados online, além da responsabilidade pelos atos cometidos no ambiente virtual.

# A pesquisa aborda as principais leis e normas que moldam a perspectiva da regulamentação do uso das tecnologias digitais, como o Marco Civil da Internet, a Lei Geral de Proteção de Dados e a Lei Contra Crimes Cibernéticos. Além disso, são discutidas as melhores práticas para garantir a privacidade e segurança dos dados dos alunos, incluindo a necessidade de proteger as informações dos alunos, utilizar plataformas seguras, garantir a autoria dos materiais e adotar medidas para evitar problemas legais.

# O objetivo geral deste projeto é realizar uma análise das implicações legais do uso de tecnologias digitais na educação, com foco em questões de privacidade, segurança de dados, direitos autorais e responsabilidade civil. Os objetivos específicos incluem identificar as principais questões legais relacionadas ao uso de tecnologias digitais na educação, analisar as leis e normas existentes que regulam o uso de tecnologias digitais na educação, identificar as melhores práticas para garantir a privacidade e segurança dos dados dos alunos, analisar os impactos dos direitos autorais no uso de materiais digitais na educação, identificar as responsabilidades legais dos envolvidos no processo educacional e propor medidas para garantir que o uso de tecnologias digitais na educação esteja em conformidade com as normas legais estabelecidas.

# Ao final, conclui-se que é fundamental uma análise cuidadosa das implicações legais do uso de tecnologias digitais na educação, para garantir que o processo educacional ocorra de forma segura e dentro das normas legais estabelecidas. A crescente digitalização da sociedade requer um direito extremamente proativo e adaptável, capaz de se antecipar às novas tendências e garantir a proteção dos direitos individuais previstos na Constituição Federal, a segurança cibernética e o desenvolvimento econômico saudável.

## Questões Legais Relacionadas ao Uso de Tecnologias na Educação

O uso de tecnologias digitais levanta uma série de questões legais complexas e em constante evolução. Com a era digital, a sociedade tem se transformado em diversos aspectos, desde as interações sociais até os modelos de negócios. Devido à velocidade com que essas transformações ocorrem, surgem grandes desafios para o sistema jurídico, que precisa se adaptar para atender às novas demandas e, consequentemente, garantir os direitos dos cidadãos. Compreender essa adaptação normativa é fundamental.

A Lei Geral de Proteção de Dados (LGPD), aprovada em 2018, estabeleceu um novo marco regulatório para a proteção de dados pessoais no Brasil, influenciado por regulamentações internacionais similares. A lei impõe regras rigorosas sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, exigindo das empresas maior transparência e responsabilidade.

Com a promulgação do Marco Civil da Internet em 2014, foram estabelecidos os princípios, garantias, direitos e deveres para o uso da Internet no Brasil. O Marco Civil da Internet é uma importante ferramenta na defesa dos direitos dos usuários no mundo virtual, garantindo a neutralidade da rede e protegendo a privacidade e os dados pessoais.

Outro fator importante está relacionado à evolução do Direito do Consumidor. A digitalização tem alterado a dinâmica de consumo. Diante do crescimento do e-commerce e das transações digitais, as normas relacionadas ao Direito do Consumidor foram adaptadas. Isso inclui o direito de arrependimento em compras online e a obrigatoriedade de que a oferta de produtos e serviços na internet seja sempre clara e transparente.

Com o crescente uso da internet, também aumentam os crimes cibernéticos. A legislação penal tem se adaptado a essa evolução, abordando os crimes que ocorrem e/ou são potencializados pelo ambiente digital. Questões como invasão de dispositivos informáticos, fraudes eletrônicas e disseminação de conteúdo malicioso agora são expressamente tipificadas.

Na área do direito civil, surgem desafios no Direito Contratual: Com a digitalização, muitos contratos são celebrados de forma eletrônica, necessitando de adaptações nas normas contratuais para garantir sua validade, autenticidade e integridade.

Diante disso, é necessária uma constante evolução na jurisprudência e a adaptação das normas vigentes. As cortes brasileiras, em particular o Supremo Tribunal Federal e os Tribunais Superiores, têm importância fundamental e vêm realizando mudanças na interpretação e adaptação das normas à realidade dessa nova era digital, consolidando entendimentos e fornecendo diretrizes para casos que surgem diariamente. Temas relacionados à inteligência artificial, internet das coisas (IoT) e blockchain apresentam novos desafios regulatórios. O direito, por sua natureza dinâmica, deve continuar a se adaptar para abordar essas e outras inovações. A crescente digitalização da sociedade requer um direito extremamente proativo e adaptável. É imperativo que o Poder Público esteja à frente dessas mudanças, compreendendo os detalhes da legislação adaptada ao caso concreto e sempre antecipando essas novas tendências.

## Leis e Normas que Regulam o Uso da Tecnologia.

De acordo com uma pesquisa realizada pelo governo brasileiro, 90% dos brasileiros têm acesso à internet em suas residências. Com o avanço da tecnologia e a customização da internet, mais pessoas têm acesso a tecnologias do que antigamente. A pesquisa aponta que de 2019 a 2021 houve um aumento de 5,8 milhões de domicílios conectados à internet, o que mostra que a cada dia mais pessoas têm acesso, trazendo benefícios, mas também problemas. Assim, é necessário regulamentar esse meio por meio de leis e medidas governamentais, para combater injustiças no âmbito digital e crimes cibernéticos.

De acordo com o cenário atual, é importante destacar que as tecnologias digitais desempenham um papel crucial na sociedade, afetando diversas esferas da vida humana, desde a comunicação até os processos produtivos. No Brasil, a regulamentação do uso dessas tecnologias visa equilibrar sua adoção com a proteção dos direitos individuais previstos na Constituição Federal, a segurança cibernética e o desenvolvimento econômico saudável. Nesse contexto, foram estabelecidas diversas leis e normas para direcionar o uso responsável das tecnologias digitais. Ao longo desta pesquisa, abordaremos as principais leis e normas que moldam essa perspectiva.

Inicialmente, é necessário embasar-se em uma lei que garanta direitos no âmbito digital, com a finalidade de evitar que certos direitos sejam feridos. Nesse sentido, surgiu a Lei 12.965/2014, conhecida como “Marco Civil da Internet”. Dentro dela, foram estabelecidos princípios, garantias, direitos e deveres para o uso da Internet no Brasil. A norma reforça a neutralidade da rede, assegurando que o tráfego de dados seja tratado de forma isonômica, sem discriminação. Além disso, o Marco Civil determina a responsabilidade dos provedores de serviços online em relação aos dados dos usuários, promovendo a privacidade e a proteção das informações pessoais.

Em uma análise mais aprofundada, em 2018 foi promulgada a Lei Geral de Proteção de Dados (Lei 13.709/2018) para proteger os direitos fundamentais de liberdade, privacidade e livre formação da personalidade de cada indivíduo. Inspirada no Regulamento Geral de Proteção de Dados da União Europeia, essa lei estabelece diretrizes sobre a coleta, armazenamento, tratamento e compartilhamento de dados pessoais. Busca-se, dessa maneira, proteger a privacidade dos cidadãos, exigindo consentimento explícito para o uso de suas informações, além de impor medidas de segurança cibernética e possibilitar que os titulares tenham controle sobre seus dados.

Além disso, a Lei Contra Crimes Cibernéticos (Lei 12.737/2012), também conhecida como "Lei Carolina Dieckmann", é uma norma de fundamental importância no combate ao crime digital, principalmente em relação às redes sociais. Essa legislação aborda delitos cometidos no ambiente digital, como invasão de dispositivos, roubo de informações e divulgação não autorizada de dados pessoais. Dessa forma, estão previstas punições para essas práticas, garantindo a segurança cibernética.

Por fim, mas não menos importante, com a regulamentação do Open Banking, por meio de resoluções do Banco Central, houve um avanço significativo no país em relação à implementação do sistema de Open Banking. Ele visa a compartilhamento seguro de dados bancários entre instituições financeiras, promovendo a concorrência, a inovação e a oferta de produtos financeiros mais diversificados.

Infere-se, portanto, que essas leis e normas representam um esforço do Brasil para estabelecer um ambiente regulatório que promova o uso responsável das tecnologias digitais, garantindo direitos individuais, segurança cibernética e desenvolvimento econômico. No entanto, é importante destacar que o cenário tecnológico está em constante evolução, exigindo uma revisão contínua das regulamentações para se adequarem aos desafios emergentes. Sendo assim, caso continuem evoluindo com mais leis e mecanismos de regulamentação, será possível falar em uma qualidade na segurança digital, tendo como objetivo o bem-estar da população e a segurança.

## Melhores Práticas para Garantir a Privacidade e Segurança dos Dados dos Alunos

As violações de privacidade na internet são perigos reais que incluem compartilhamento de dados pessoais sem permissão, roubo de identidade e disponibilização de informações a pessoas mal intencionadas. Embora as pessoas estejam cada vez mais conscientes desses riscos, a proteção da privacidade na internet ultrapassa a proteção de dados bancários ou perfis em redes sociais. Sempre que visitamos um site ou baixamos um aplicativo, nossos dados são armazenados, geralmente sem consentimento e sem nosso conhecimento. A privacidade na web é importante porque permite gerenciar para onde esses dados vão e como serão usados, permitindo que cada um decida se quer evitar que eles sejam coletados completamente ou parcialmente. Nesse sentido, a Lei Geral de Proteção de Dados (LGPD) foi sancionada com o propósito de proteger os dados de pessoas e empresas, oferecendo maior autonomia às pessoas acerca de seus dados pessoais. A LGPD visa proteger internautas da violação de suas informações e garantir o cumprimento da legislação em relação à coleta, armazenamento, tratamento e compartilhamento de dados pessoais.

A Lei Geral de Proteção de Dados (LGPD) exige que as empresas sigam regras para tornar mais seguro o compartilhamento de dados dos usuários, protegendo informações como nome, documentos pessoais, endereço, email e telefone. O descumprimento dessa lei pode resultar em prejuízos financeiros para a empresa, além de abalar significativamente sua reputação no mercado. Por isso, é cada vez mais comum que organizações mapeiem riscos de vazamento de dados e violações de privacidade a fim de evitar incidentes negativos na segurança. É importante lembrar que a adequação à LGPD é uma exigência legal que pode incorrer em sanções por seu descumprimento, sendo ela a principal forma de proteger empresas, instituições ou organizações.

Mesmo com as instituições adotando medidas preventivas, problemas como vazamentos de dados ainda são passíveis de ocorrer. Para lidar com essas situações, é necessário ter um plano de resposta a incidentes que avalie aspectos importantes para a resolução do ocorrido, como detectar a origem do vazamento, coletar evidências sobre o fato, evitar duplicações de dados, entender o tracking, encontrar logs de rastreabilidade e fazer uma revisão das permissões de acesso.

Para se prevenir de situações de vazamento de dados, é importante proteger tanto as suas comunicações pela internet quanto seus dispositivos utilizados para acessá-la, sejam notebooks, PCs, smartphones ou tablets. Privacidade e segurança on-line andam de mãos dadas, e tomar medidas para protegê-las é um passo significativo para evitar possíveis problemas.

## Impacto dos Direitos Autorais na Educação

Os direitos autorais desempenham um papel fundamental no uso de materiais digitais na educação, e suas implicações podem ser complexas e variadas.

O acesso a materiais como livros, artigos, vídeos e software protegidos por direitos autorais é frequentemente restrito. Isso pode limitar o acesso a esses recursos, especialmente se eles não estiverem disponíveis gratuitamente ou sob licenças de uso flexíveis, como Creative Commons.

Em muitos países, existe o conceito de "uso justo" (fair use em inglês), que permite o uso limitado de materiais protegidos por direitos autorais sem a permissão do titular dos direitos. No entanto, os limites do uso justo podem ser ambíguos e variar de acordo com a jurisdição, tornando difícil determinar o que é permitido.

Uma resposta à restrição dos direitos autorais é a promoção dos Recursos Educacionais Abertos (REA). Estes são materiais de ensino, aprendizado e pesquisa que são disponibilizados gratuitamente e, muitas vezes, sob licenças flexíveis que permitem o uso, adaptação e distribuição.

As leis de direitos autorais estão em constante evolução para se adaptarem ao ambiente digital em rápida mudança. Isso pode trazer tanto benefícios quanto desafios para o uso de materiais digitais na educação, dependendo das políticas governamentais e das decisões judiciais

No Brasil, a principal lei que trata dos direitos autorais é a Lei de Direitos Autorais, Lei nº 9.610/1998. Embora tenha sido promulgada antes da era digital, foi posteriormente atualizada para considerar os desafios e oportunidades apresentados pela distribuição de conteúdo digital.

A Lei de Direitos Autorais do Brasil protege obras digitais, incluindo livros eletrônicos, músicas em formato digital, vídeos, software e outras criações intelectuais digitais da mesma forma que as obras tradicionais.

A lei brasileira estabelece os direitos exclusivos dos detentores de direitos autorais, como o direito de reprodução, distribuição, adaptação e comunicação ao público. No entanto, também prevê exceções e limitações, como o uso justo, que permite a utilização de obras protegidas sob certas condições.

Os Provedores de Serviços de Internet (ISPs) têm a responsabilidade de tomar medidas para coibir a violação de direitos autorais em suas plataformas. Isso inclui a remoção de conteúdo infrator e a possibilidade de punição em caso de não conformidade.

A lei brasileira permite o uso de tecnologias de Gestão de Direitos Autorais Digitais (DRM) para proteger obras digitais, desde que essas tecnologias estejam em conformidade com a legislação e não impeçam o uso justo de obras protegidas. Ela reconhece a importância do licenciamento de conteúdo digital e fornece diretrizes para a negociação e uso de licenças digitais.

É importante destacar que a legislação de direitos autorais pode ser complexa e está em constante evolução, especialmente em resposta às mudanças tecnológicas. O Brasil é signatário de tratados internacionais de direitos autorais que influenciam sua legislação, como o Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio (TRIPS) da Organização Mundial do Comércio (OMC).

## Responsabilidades Legais dos Envolvidos no Processo Educacional

A era digital trouxe consigo uma série de desafios para os mais diversos contextos de convivência social e educacional. Esses desafios estão relacionados às mudanças no modo como os estudantes aprendem, interagem e acessam informações. A ideia de ‘sociedade da informação’ e de ‘cidadania digital’ está ganhando contornos de difícil controle. Nesse sentido, o legislador tem buscado proteger os direitos básicos dos cidadãos por meio da Lei Geral de Proteção de Dados Pessoais (Lei. Nº 13.709/20218, LGPD), além de órgãos de natureza normativa como a Associação Brasileira de Normas Técnicas (ABNT) que traz uma grande contribuição para uma política de segurança da informação, mormente em ambiente de publicações acadêmicas.

O compromisso da legislação em assegurar os direitos à informação, à intimidade, à privacidade bem como outros, decorrentes do tratamento de dados sensíveis assegurados no artigo 5° da LGPD, é decorrente da ligação direta com a personalidade do indivíduo. Essas informações relevantes compõem o arcabouço de valores que impulsionam as atividades acadêmicas, uma vez que são imprescindíveis para que os serviços e produtos educacionais contribuam com o desenvolvimento educacional e tecnológico do país.

O gestor na adoção de medidas de proteção das informações relativas a dados pessoais deve considerar, além da importância dessas para o sucesso do negócio, o risco de danos consideráveis para o titular dos direitos. As consequências envolvem diversos direitos, inclusive a dignidade da pessoa humana, que venha a ter seus dados vulnerados e a própria imagem da instituição no mercado. Nesse sentido, as recentes produções legislativas brasileiras têm contribuído para proteger os dados das pessoas físicas e jurídicas, consubstanciando um ambiente de segurança jurídica para os usuários dos serviços.

Com o crescente incremento do ensino remoto nas instituições educacionais durante a pandemia, há várias questões de segurança que precisam ser esclarecidas. Entre elas, pode-se destacar a responsabilidade das instituições no tratamento de dados sensíveis dos usuários e dos profissionais que não foram tecnicamente preparados para atuar de forma remota. Nesse cenário, surgiu a necessidade de adequação dos meios didáticos para o melhor aproveitamento das ferramentas empregadas e a manutenção dos padrões de qualidade do ensino oferecido em níveis aceitáveis, mas a segurança das informações permeia todo esse processo e exige uma política adequada de uso e proteção dados.

Nesse cenário, o papel dos profissionais envolvidas ganha relevância na medida em que há uma consciência de combate a fraudes, desinformações e espaço para desenvolvimento de políticas de segurança, sejam em âmbito escolar ou universitário. A facilidade de copiar e colar informações da internet apresenta o desafio do plágio acadêmico, bem como outras práticas que põem xeque a lisura com que foram produzidas as informações. Os estudantes precisam compreender os princípios de autoria, citar corretamente suas fontes e desenvolver o pensamento crítico para criar trabalhos autênticos.

Nesse contexto, os órgãos normativos - públicos e privados - devem estabelecer políticas de controle de qualidade e segurança em todas as fases de manuseio da informação, de forma especial, os dados manipulados digitalmente. A segurança online é uma preocupação crescente em todos cenários que se imagina em uma sociedade dominada por meios de comunicação. Assim, a temática de ampliação de acesso à educação por meio da rede mundial de computadores, em um país de extensão continental como o Brasil, requer medidas de grande amplitude e alcance de estudantes e instituições que enfrentam obstáculos relacionados à proteção de dados pessoais, prevenção de ataques cibernéticos e garantia da privacidade online.

### O papel do professor na educação na era digital

A cidadania digital abrange um conjunto de competências e habilidades que vão além do mero conhecimento técnico. Ela engloba a capacidade de discernir informações confiáveis, avaliar criticamente conteúdos online, proteger a privacidade e a segurança pessoal, além de desenvolver relações saudáveis e éticas nas interações digitais. Essas competências são essenciais para a plena participação e engajamento dos indivíduos na sociedade digital.

As transformações das sociedades digitais contemporâneas foram marcadas pela evolução das tecnologias da informação e da comunicação: o espaço virtual se tornou um lugar de se exercitar a cidadania por meio de troca de informações e opiniões com uma velocidade jamais imaginada. O legislador pátrio, percebendo essa grande mudança, criou um arcabouço normativo para orientar órgãos, empresas públicas e privadas a tratar os dados pessoais observando os ditames normativos, como prevê o artigo 2º da LGPD.

No âmbito do ensino, os profissionais da educação superior e básica têm grande papel na educação para coibir práticas danosas ao ensino remoto de forma segura. Um dos objetivos é orientar sobre a importância da educação para a cidadania digital no ensino básico e superior, fortalecendo a formação de estudantes como cidadãos digitais responsáveis e engajados com políticas de proteção dados conforme os ditames legais.

Diversos estudiosos têm abordado o tema da educação para a cidadania digital e destacado a importância do papel dos profissionais da educação nesse contexto. Autores como Ribble, Bailey, e Lindsay (2011) argumentam que a cidadania digital é essencial para a participação plena e efetiva na sociedade contemporânea. Eles ressaltam a importância de desenvolver competências digitais, como pensamento crítico, respeito pela privacidade e segurança online, além da habilidade de avaliar e utilizar de forma ética as informações disponíveis. Os profissionais da educação são os principais mediadores entre os estudantes e as tecnologias, orientando-os no desenvolvimento de habilidades e valores necessários para uma cidadania responsável.

Embora de difícil definição na prática, a cidadania digital trouxe vários desafios para o ensino-aprendizagem no contexto das tecnologias que segundo Sharpe (2010) “Os desafios incluem a necessidade de promover o letramento digital entre alunos e professores, desenvolver programas de formação docente para lidar com as demandas tecnológicas e garantir a acessibilidade e inclusão digital para todos os estudantes”. Alguns desses desafios são:

Segurança digital: A segurança online é uma preocupação crescente no contexto de ensino-aprendizagem em especial, no mediado por recursos tecnologias. Os estudantes e as instituições enfrentam desafios relacionados à proteção de dados pessoais, prevenção de ataques cibernéticos e garantia da privacidade online;

Mudança no papel do professor: A era digital também desafia o papel tradicional do professor. Os educadores precisam se adaptar a novas formas de ensino e aprendizagem, incorporando tecnologias digitais em suas práticas pedagógicas e promovendo a participação ativa dos estudantes.

Desigualdade de acesso: Nem todos os estudantes têm acesso igual às tecnologias e à internet. Isso pode criar disparidades no acesso a recursos educacionais e oportunidades de aprendizagem online, aprofundando a divisão digital entre os estudantes. Aliado a essas desigualdades, há que se ressaltar a necessidade de inclusão das pessoas por meio de políticas de segurança digital;

Plágio e autenticidade: A facilidade de copiar e colar informações da internet apresenta o desafio do plágio acadêmico, além do excesso de informações que nem sempre é seguido por um filtro adequado. Nesse cenário, a divulgação de notícias falsas (fake news) é outro problema relacionada a produção de informações baseadas em fontes que não são fidedignas. Os estudantes precisam compreender os princípios de autoria, citar corretamente suas fontes e desenvolver o pensamento crítico para criar trabalhos autênticos.

## Considerações finais

Há um enorme universo a ser desbravado pelos professores e instituições educacionais na seara da proteção digital. Os diplomas normativos (Lei 12.965/2013, Marco Civil da internet e 13.709 de 2018, LGPD) trazem bases sólidas para se iniciar um trabalho que busque acompanhar a evolução das tecnologias aplicadas na ampliação do acesso à educação na era digital. Os profissionais da educação podem assumir a dianteira na construção de discussões que estimulem os alunos a refletir sobre as implicações sociais, éticas e legais do uso da tecnologia. Esses debates podem abordar tópicos como privacidade, liberdade de expressão, desigualdades digitais, *fake news* e impacto dos recursos digitais na sociedade.

Enfrentar questões dessa natureza requer uma abordagem abrangente, envolvendo tanto os estudantes quanto as instituições educacionais. É necessário promover a educação digital aliada às políticas de segurança cibernética, oferecer suporte aos estudantes na aquisição de habilidades digitais e éticas, e adaptar as práticas pedagógicas para aproveitar ao máximo as oportunidades oferecidas pelos recursos tecnológicos disponíveis.

Referências

Nhancale, Cláudio Ângelo, *et al*. "Educação para a cidadania digital: o papel do professor universitário no contexto atual." *Revista Multidisciplinar do Nordeste Mineiro* 7.1 (2023).

Martirena, Ricardo Pedroza. "A proteção de dados pessoais e da propriedade intelectual no ensino remoto: estudo de caso no Centro Universitário Uniprojeção." (2022).

RIBBLE, M. Digital Citizenship in Schools: Nine Elements All Students Should Know. International Society for Technology in Education. (2011). SEVERINO, Antônio Joaquim. Metodologia do trabalho científico. 21. Ed. São Paulo: Cortez 2000.

SHARPE, R., Beetham, H., & De Freitas, S. Rethinking Learning for a Digital Age: How Learners are Shaping their Own Experiences. Routledge. (2010).

DO CARMO FIGUEIREDO, Adriana, et al. *TECNOLOGIA E RESPONSABILIDADE: reflexões éticas, jurídicas e educacionais*. Editora BAGAI, 2021.