DA TUTELA DA IMAGEM E PRIVACIDADE NO ESPAÇO DIGITAL SOB O ENFOQUE DOS DIREITOS HUMANOS NA ERA DA TECNOLOGIA

Thiago Bica Esteves

RESUMO:

O presente artigo visa abordar a crescente importância da proteção da imagem e privacidade das pessoas no contexto do ambiente digital, sob a perspectiva dos direitos humanos. Com o avanço tecnológico e a proliferação das redes sociais e plataformas online, surgem desafios significativos para garantir a preservação dos direitos individuais. A proteção da imagem e privacidade tornou-se uma questão crucial, considerando a facilidade com que informações e imagens pessoais podem ser compartilhadas e acessadas globalmente. O estudo analisa a legislação nacional relacionada à proteção da imagem e privacidade, destacando as lacunas e desafios enfrentados na aplicação dessas leis no ambiente digital. Além disso, são discutidos casos emblemáticos que evidenciam violações dos direitos humanos no espaço digital, incluindo a disseminação não autorizada de imagens íntimas, o *cyberbullying* e as *deepfakes.* Ao mesmo tempo, são exploradas as possíveis soluções para mitigar tais problemas, incluindo a adoção de legislação mais abrangente e eficaz, o fortalecimento dos mecanismos de proteção de dados pessoais e a promoção da conscientização sobre os direitos digitais entre os usuários. Destaca-se a necessidade de uma abordagem holística e colaborativa envolvendo governos, empresas de tecnologia e sociedade civil para enfrentar os desafios emergentes relacionados à tutela da imagem e privacidade no espaço digital. Em última análise, o artigo ressalta a importância de se proteger os direitos humanos fundamentais no cenário digital, garantindo que o avanço tecnológico não comprometa a dignidade e a liberdade das pessoas.

Palavras-chave: inteligência artificial, privacidade, imagem, direitos humanos.

ABSTRACT

This article aims to address the growing importance of protecting people's image and privacy in the context of the digital environment, from the perspective of human rights. With technological advancement and the proliferation of social networks and online platforms, significant challenges arise in ensuring the preservation of individual rights. Image and privacy protection has become a crucial issue, considering the ease with which personal information and images can be shared and accessed globally. The study analyzes national legislation related to image protection and privacy, highlighting the gaps and challenges faced in the application of these laws in the digital environment. Furthermore, emblematic cases are discussed that highlight human rights violations in the digital space, including the unauthorized dissemination of intimate images, cyberbullying and deepfakes. At the same time, possible solutions to mitigate such problems are explored, including adopting more comprehensive and effective legislation, strengthening personal data protection mechanisms and promoting awareness of digital rights among users. The need for a holistic and collaborative approach involving

governments, technology companies and civil society is highlighted to face emerging challenges related to the protection of image and privacy in the digital space. Ultimately, the article highlights the importance of protecting fundamental human rights in the digital scenario, ensuring that technological advances do not compromise people's dignity and freedom.

Keywords: artificial intelligence, privacy, image, human rights.

INTRODUÇÃO

Nos últimos anos da década de 2010, a era digital presenciou uma revolução sem precedentes impulsionada pelo avanço exponencial da tecnologia digital. A internet e suas plataformas, redes sociais, dispositivos móveis e outras inovações têm transformado fundamentalmente a forma como as pessoas se comunicam, interagem e compartilham informações. Neste cenário em constante evolução tecnológica, surgem questões complexas e urgentes relacionadas à proteção da imagem e da privacidade dos indivíduos no espaço digital.

Este artigo se propõe a explorar em profundidade a interseção entre a tutela da imagem, a privacidade e os direitos humanos na era digital. O enfoque é analisar como os avanços tecnológicos têm impactado esses direitos fundamentais, bem como examinar as estratégias legais, éticas e sociais necessárias para garantir uma proteção eficaz no ambiente digital.

No contexto contemporâneo, onde a tecnologia permeia todos os aspectos da vida individual cotidiana, a noção de privacidade e imagem está em constante redefinição. As fronteiras entre o público e o privado tornam-se cada vez mais difusas, à medida que as informações pessoais são coletadas, armazenadas e compartilhadas em uma escala sem precedentes. O surgimento de tecnologias como a inteligência artificial, reconhecimento facial e análise de *big data* adiciona camadas adicionais de complexidade a essa equação, levantando preocupações sobre vigilância em massa, discriminação algorítmica e violações de privacidade em larga escala.

Neste contexto, os direitos humanos emergem como um referencial essencial para avaliar e enfrentar os desafios da era digital. A Declaração Universal dos Direitos Humanos proclama o direito à privacidade e à liberdade de expressão como fundamentais para a dignidade e o bem-estar humanos. No entanto, a aplicação desses princípios no contexto digital enfrenta obstáculos significativos, incluindo lacunas regulatórias, interesses conflitantes entre

empresas e indivíduos, e uma compreensão em constante mutação das dinâmicas sociais e éticas da tecnologia.

Ao longo deste artigo, serão explorados diversos aspectos relacionados à tutela da imagem e privacidade no espaço digital sob a ótica dos direitos humanos. Inicialmente, será examinado os fundamentos teóricos desses direitos, contextualizando-os no cenário contemporâneo da tecnologia digital. Em seguida, abordar-se-á os principais desafios e dilemas éticos enfrentados na proteção da imagem e privacidade online, destacando casos emblemáticos e tendências emergentes.

Partindo de uma abordagem interdisciplinar, combinando elementos do direito, ética, sociologia e tecnologia, este estudo pretende oferecer uma visão abrangente e equilibrada das questões em pauta. Além disso, será dada atenção especial às estratégias e soluções propostas por governos, organizações da sociedade civil, empresas e indivíduos para enfrentar esses desafios de forma eficaz e compatível com os princípios dos direitos humanos.

Por fim, este artigo visa contribuir para um debate informado e construtivo sobre como conciliar os imperativos da tecnologia digital com a proteção dos direitos humanos fundamentais. Ao destacar os princípios orientadores e as melhores práticas nesta área, pretende-se oferecer *insights* valiosos para a formulação de políticas públicas, regulamentações e práticas empresariais que promovam uma cultura digital baseada no respeito à dignidade e à autonomia dos indivíduos.

1 TEORIA GERAL DOS DIREITOS HUMANOS

A teoria geral dos direitos humanos é um campo multidisciplinar que busca compreender a natureza, fundamentos, desenvolvimento e aplicação dos direitos humanos. Esta teoria fornece uma estrutura conceitual e normativa para entender a natureza e o alcance dos direitos humanos, bem como os princípios subjacentes que os fundamentam.

Existem várias abordagens e perspectivas na teoria geral dos direitos humanos, que podem incluir elementos filosóficos, jurídicos, políticos, sociológicos e históricos. Algumas das questões fundamentais abordadas por essa teoria incluem:

No que diz respeito a natureza jurídica dos direitos humanos, essa questão debate se os direitos humanos são inerentes à condição humana ou se são construções sociais e culturais. Também explora se os direitos humanos são absolutos ou relativos, universais ou culturalmente relativos (ELIAS *et al*, 2019).

As origens e fundamentos examinam as origens históricas dos direitos humanos, desde a sua evolução nas tradições filosóficas e religiosas até as declarações formais de direitos humanos, como a Declaração Universal dos Direitos Humanos de 1948. As **a**bordagens jurídicas analisam o papel do direito internacional dos direitos humanos, bem como a incorporação dos direitos humanos nas constituições nacionais e sistemas legais domésticos. Explora também os mecanismos de aplicação e proteção dos direitos humanos, incluindo tribunais internacionais e regionais (ELIAS *et al*, 2019).

Quanto a dimensão política e social, se considera o impacto das estruturas de poder, desigualdades sociais e políticas públicas na efetivação dos direitos humanos. Examina questões como justiça social, distribuição de recursos e participação política. O desenvolvimento e evolução histórica estuda como os direitos humanos têm evoluído ao longo do tempo em resposta a mudanças sociais, culturais, econômicas e políticas. Também explora os desafios contemporâneos enfrentados pelos direitos humanos em um mundo globalizado e interconectado (PIOVESAN, 2009).

Por fim, a discussão da Universalidade versus Relativismo, debate a questão de se os direitos humanos devem ser aplicados de forma uniforme em todas as culturas e contextos ou se devem ser adaptados às particularidades culturais e sociais de cada sociedade (ELIAS *et al*, 2019).

1.1 Do Conceito de Direitos Humanos

Os direitos humanos são um conjunto de normas, princípios e valores fundamentais reconhecidos internacionalmente que visam proteger e garantir a dignidade, liberdade e igualdade de todos os seres humanos, independentemente de sua origem, raça, sexo, religião, opinião política, entre outras características. Esses direitos são inerentes a todos os indivíduos pelo simples fato de serem humanos e são considerados universais, inalienáveis, interdependentes e indivisíveis (NAÇÕES UNIDAS, 1948):

Universais: Os direitos humanos são aplicáveis a todas as pessoas, em todos os lugares, independentemente de fronteiras nacionais. Eles são considerados como pertencendo a todos os seres humanos, simplesmente por sua condição de seres humanos (NAÇÕES UNIDAS, 1948).

Inalienáveis: Os direitos humanos são intransferíveis e não podem ser retirados ou violados sob nenhuma circunstância. Eles são intrínsecos à pessoa e não podem ser negociados ou renunciados (NAÇÕES UNIDAS, 1948).

Interdependentes e indivisíveis: Os diferentes direitos humanos estão interligados e são igualmente importantes. O respeito por um direito muitas vezes está ligado ao respeito por outros direitos. Por exemplo, o direito à saúde está relacionado ao direito à vida e à dignidade (PIOVESAN, 2009).

Dignidade e Igualdade: Os direitos humanos visam proteger a dignidade de todos os indivíduos, garantindo-lhes igualdade de tratamento e oportunidades, independentemente de suas características pessoais ou sociais (NAÇÕES UNIDAS, 1948).

Os direitos humanos abrangem uma variedade de áreas, incluindo direitos civis e políticos (como liberdade de expressão, liberdade de religião e direito à privacidade), direitos econômicos, sociais e culturais (como direito à educação, trabalho digno e saúde), bem como direitos coletivos, como o direito à autodeterminação e à participação política. Esses direitos são formalizados em documentos internacionais, como a Declaração Universal dos Direitos Humanos (DUDH), adotada pela Assembleia Geral das Nações Unidas em 1948, e são posteriormente desenvolvidos e detalhados em tratados internacionais e regionais de direitos humanos. A promoção e proteção dos direitos humanos são essenciais para a construção de sociedades justas, pacíficas e inclusivas, e são fundamentais para o desenvolvimento humano sustentável.

1.2 Das gerações/dimensões dos Direitos Humanos

Os direitos humanos são frequentemente categorizados em diferentes "gerações" ou "dimensões" para refletir a evolução histórica e a ampliação do escopo desses direitos ao longo do tempo. Essa classificação em gerações/dimensões ajuda a compreender melhor a natureza e a abrangência dos direitos humanos em diferentes contextos. As três principais gerações ou dimensões dos direitos humanos serão expostas adiante.

1.2.1 Primeira Dimensão/Geração: Liberdades Clássicas

Essa dimensão abrange direitos individuais que são tradicionalmente associados à ideia de liberdade e autonomia individual. Incluem direitos como liberdade de expressão, liberdade de religião, direito à vida, liberdade de reunião, direito a um julgamento justo, entre outros.

Esses direitos foram promovidos principalmente no contexto das revoluções liberais dos séculos XVIII e XIX, destacando a importância de proteger os indivíduos contra a opressão do Estado e garantir sua participação na vida política (BOSCIONI, 2024).

1.2.2 Segunda Dimensão/Geração: Direitos Econômicos, Sociais e Culturais

Esta dimensão está preocupada com os direitos que visam garantir o bem-estar socioeconômico e a igualdade material entre os indivíduos. Incluem direitos como o direito ao trabalho digno, direito à educação, direito à saúde, direito à moradia, entre outros (BOSCIONI, 2024).

Esses direitos surgiram como resposta às condições de exploração e desigualdade econômica geradas pela Revolução Industrial, com o reconhecimento de que a liberdade civil não é suficiente para garantir a dignidade humana sem garantias sociais (BOSCIONI, 2024).

1.3.3 Terceira Dimensão/Geração: Direitos Coletivos, Solidários e Ambientais

Esta dimensão aborda os direitos que estão relacionados ao bem-estar de grupos de pessoas, bem como ao meio ambiente. Incluem direitos como o direito à autodeterminação dos povos, direito ao desenvolvimento, direito à paz, direito a um ambiente saudável, entre outros (BOSCIONI, 2024).

Esses direitos emergiram em resposta às demandas por justiça global, sustentabilidade ambiental e reconhecimento dos direitos das comunidades e povos indígenas. É importante ressaltar que essa divisão em gerações/dimensões não implica em uma hierarquia entre os direitos, mas sim em uma complementaridade. Todos os direitos humanos são interdependentes e indivisíveis, e sua realização plena requer a promoção e proteção de todas as dimensões. Além disso, novos desafios e questões emergentes, como os direitos digitais e o direito à paz, continuam a moldar a evolução dos direitos humanos (BOSCIONI, 2024).

2 DO DIREITO À IMAGEM, HONRA E PRIVACIDADE

O direito à imagem, honra e privacidade são componentes essenciais dos direitos individuais e são protegidos em várias jurisdições ao redor do mundo, muitas vezes através de leis específicas ou de disposições dentro do direito civil.

Direito à Imagem: Este direito protege a representação visual de uma pessoa, seja através de fotografias, vídeos, pinturas, ou qualquer outra forma de representação gráfica. Em muitos países, o direito à imagem permite que uma pessoa controle o uso de sua imagem para

evitar exploração comercial sem consentimento, bem como para proteger sua dignidade e identidade. Isso significa que a utilização da imagem de uma pessoa para fins comerciais ou publicitários geralmente requer consentimento prévio, a menos que esteja amparada por exceções legais, como o uso em contexto jornalístico ou artístico (TRABALLI, 2016).

Direito à Honra: Este direito refere-se à proteção da reputação e integridade moral de uma pessoa contra-ataques injustos ou difamatórios. Isso inclui a proteção contra declarações falsas que possam prejudicar a reputação de alguém, bem como contra invasões injustificadas de privacidade que possam causar dano à sua dignidade ou reputação (TRABALLI, 2016).

Direito à Privacidade: Este direito protege a capacidade de uma pessoa controlar informações sobre si mesma e decidir como essas informações são compartilhadas e utilizadas por outros. Isso abrange uma ampla gama de aspectos da vida pessoal, incluindo informações médicas, financeiras, familiares, e outros detalhes íntimos. A privacidade também se estende à proteção do espaço físico, como a casa de uma pessoa, contra intrusões não autorizadas (TRABALLI, 2016).

É importante notar que esses direitos podem entrar em conflito com outros direitos, como a liberdade de expressão e o interesse público. Portanto, é frequentemente necessário equilibrar esses direitos em casos em que há confronto. Os tribunais geralmente consideram vários fatores, como o contexto em que a informação foi divulgada, a importância do interesse público envolvido e o impacto na vida da pessoa afetada, ao decidir sobre casos que envolvem direitos de imagem, honra e privacidade.

A análise constitucional do direito à imagem, honra e privacidade varia de acordo com a constituição de cada país. No entanto, é possível fornecer uma análise geral, destacando como esses direitos são protegidos em muitas constituições ao redor do mundo.

O direito à imagem, em várias constituições, é implicitamente protegido como parte do direito à vida privada. Por exemplo, na Constituição Federal do Brasil de 1988, o direito à intimidade e à vida privada é garantido pelo artigo 5º, inciso X. Isso inclui o direito de controlar a própria imagem. Além disso, o direito à imagem pode ser protegido por meio de leis específicas que regulam o uso comercial e não comercial da imagem de uma pessoa (MORAES, 2009).

Já o Direito à Honra, geralmente é protegido por disposições constitucionais que garantem a dignidade humana e a integridade pessoal. Por exemplo, na Constituição Espanhola

de 1978, o artigo 18 estabelece que "a lei limitará o uso da informática para garantir o honor e a intimidade pessoal e familiar dos cidadãos e o pleno exercício de seus direitos". Isso implica que qualquer violação à honra de uma pessoa pode ser objeto de proteção constitucional e legal (FRANCIULLI, 2004).

Por fim, o direito à privacidade é frequentemente protegido por constituições de maneira explícita, como parte do direito à vida privada, ou de maneira implícita, através da proteção contra invasões arbitrárias do espaço privado. Por exemplo, na Constituição dos Estados Unidos, embora o termo "privacidade" não esteja explicitamente mencionado, a Suprema Corte dos Estados Unidos interpretou que várias disposições constitucionais, como a Quarta Emenda, garantem um "direito à privacidade". Da mesma forma, a Constituição da Índia protege a privacidade como parte do direito à vida e à liberdade pessoal (LUIZA, 2023).

Em geral, a análise constitucional desses direitos envolve a interpretação de disposições constitucionais relevantes à luz dos princípios fundamentais da dignidade humana, liberdade individual e justiça. Os tribunais muitas vezes são chamados a equilibrar esses direitos com outros direitos fundamentais, como a liberdade de expressão, de forma a garantir um equilíbrio justo e razoável entre os interesses em pauta.

3 DA TUTELA DA IMAGEM E PRIVACIDADE NO ESPAÇO DIGITAL

A proteção da imagem e da privacidade no espaço digital emerge como um tema de extrema relevância no contexto contemporâneo. O avanço tecnológico e a proliferação das mídias digitais têm desencadeado uma série de desafios e dilemas éticos relacionados à exposição e controle das informações pessoais online. Nesse sentido, é fundamental compreender as dinâmicas complexas que permeiam essa questão e explorar as estratégias necessárias para garantir uma tutela eficaz dos direitos fundamentais dos indivíduos.

Uma das principais preocupações diz respeito à coleta indiscriminada e ao uso indevido de dados pessoais por parte de empresas, governos e outras entidades. Com o advento da internet e das redes sociais, as informações privadas dos usuários tornaram-se um recurso valioso, frequentemente explorado para fins comerciais, políticos e até mesmo criminais. Nesse contexto, visando que a IA não ultrapasse essas barreiras da integridade, segundo Floridi (2021), em entrevista concedida ao Instituto Humanitas Unisinos, o Filósofo enfatizou que há a extrema necessidade de garantir que sistemas de IA respeitem os direitos fundamentais dos indivíduos, incluindo o direito à privacidade e o controle sobre sua imagem e segurança. Pois

a falta de controle sobre esses dados pode resultar em violações graves da privacidade e em potenciais danos à reputação e bem-estar dos indivíduos.

Além disso, a disseminação de imagens e vídeos na internet levanta questões específicas relacionadas à proteção da imagem e identidade pessoal. A facilidade com que conteúdos podem ser compartilhados e replicados online aumenta o risco de exposição não autorizada e manipulação digital, colocando em xeque a integridade e autenticidade das representações digitais das pessoas. Essa realidade é especialmente preocupante no contexto de *cyberbullying*, pornografia de vingança e outros tipos de abusos que podem ter consequências devastadoras para as vítimas. Como exemplo destes casos, tem-se o ocorrido com a atriz e apresentadora Carolina Dieckmann, exemplo notório de violação de privacidade e imagem no contexto digital. Em 2012, a atriz brasileira teve seu computador pessoal hackeado, resultando no vazamento de fotos íntimas e pessoais. As imagens foram compartilhadas na internet sem o consentimento da vítima, gerando uma grande repercussão na mídia e levantando questões sobre segurança digital e proteção da privacidade (ARAÚJO, 2023).

O incidente envolvendo Carolina Dieckmann despertou debates sobre os limites da privacidade no ambiente online e a necessidade de medidas mais rigorosas para proteger os indivíduos contra violações desse tipo. O caso também evidenciou os riscos associados ao armazenamento e compartilhamento de informações pessoais na era digital, destacando a importância da conscientização e educação digital para prevenir esse tipo de crime cibernético. Consoante ao ocorrido, foi sancionada pela então presidente da República, Dilma Rousseff, a Lei n° 12.737/2012, que tipificou no código penal o crime de invasão de dispositivo informático, sendo eles, celulares, computadores, notebooks, tablets etc.

Não obstante, o caso das *deepfakes* envolvendo Barack Obama e Donald Trump exemplifica os desafios emergentes relacionados à manipulação de conteúdo e informações no ambiente digital. Deepfakes são vídeos manipulados por inteligência artificial que podem fazer com que uma pessoa pareça dizer ou fazer algo que nunca disse ou fez na realidade. Em 2018, um vídeo *deepfake* de Barack Obama foi amplamente divulgado, onde ele parecia fazer declarações falsas e comprometedoras (*Vídeos falsos e deepfakes – como os usuários podem se proteger*, s.d).

Posteriormente, em 2020, um vídeo *deepfake* de Joe Biden também ganhou destaque, mostrando-o fazendo um discurso fictício incentivando a população a não participar das eleições. Ambos os casos despertaram preocupações sobre a disseminação de informações

falsas e a manipulação da opinião pública por meio de tecnologias de manipulação de vídeo cada vez mais sofisticadas (CNN, 2020).

Esses casos destacam os riscos associados à proliferação de *deepfakes* e a necessidade de medidas para detectar e combater a disseminação de conteúdo falso. Além disso, evidenciam a importância de promover a alfabetização digital e a conscientização sobre os perigos da desinformação online. O caso das *deepfakes* de Obama e Trump serve como um alerta sobre os desafios que a sociedade enfrenta na era da informação digital e a urgência de encontrar soluções eficazes para proteger a integridade e autenticidade das informações na internet.

Nesse diapasão, a tutela da imagem e privacidade no espaço digital é uma preocupação crescente em uma era onde a tecnologia permeia todos os aspectos da vida cotidiana. Para compreender melhor esse fenômeno e suas implicações, é fundamental analisar casos práticos reais que ilustram os desafios e dilemas enfrentados pelos indivíduos e pela sociedade como um todo.

Um exemplo emblemático é o caso do escândalo Cambridge Analytica, que veio à tona em 2018 e revelou a extensão do uso indevido de dados pessoais para influenciar eleições. A empresa Cambridge Analytica, por meio de uma aplicação de teste de personalidade no Facebook, coletou dados de milhões de usuários sem o seu consentimento e os utilizou para criar perfis psicológicos detalhados. Essas informações foram posteriormente utilizadas para direcionar campanhas políticas altamente segmentadas, levantando sérias preocupações sobre privacidade, manipulação de dados e interferência nas eleições democráticas (BBC NEWS, 2018).

Outro exemplo notório é o fenômeno da "pornografia de vingança", onde indivíduos têm suas imagens íntimas compartilhadas online sem o seu consentimento, muitas vezes como forma de retaliação por términos de relacionamentos ou desavenças pessoais. Um caso amplamente divulgado foi o da atriz Jennifer Lawrence e outras celebridades, cujas fotos íntimas foram hackeadas e disseminadas na internet em 2014 (EL PAÍS, 2014). Esse tipo de violação não apenas expõe a intimidade das vítimas, mas também pode causar danos emocionais, profissionais e sociais significativos, além de afetar a segurança que o indivíduo possui na própria privacidade, como leciona Carlos Affonso Souza:

> Privacidade é essencial num futuro no qual nós imaginamos que o desenvolvimento de inteligência artificial, algoritmos em geral, estarão baseados em rotinas, hábitos, usos, costumes, formas de vida que são essencialmente humanas (2019).

Além disso, as redes sociais têm sido palco de casos de *cyberbullying*, onde indivíduos são alvo de ataques verbais, difamação e assédio online. Um exemplo é o caso de Amanda Todd, uma adolescente canadense que cometeu suicídio em 2012 após ser vítima de bullying online e offline. O caso de Amanda Todd chamou a atenção para os efeitos devastadores do cyberbullying e destacou a necessidade urgente de proteger os jovens no espaço digital (MARINHO, 2019).

No contexto corporativo, vários casos demonstram os riscos associados à falta de proteção da privacidade dos dados dos consumidores. Um exemplo é o incidente de violação de dados da Equifax em 2017, onde informações pessoais de mais de 147 milhões de consumidores foram comprometidas devido a falhas de segurança na empresa. Essa violação expôs os indivíduos a riscos de roubo de identidade, fraude financeira e outros tipos de crimes cibernéticos, evidenciando a importância de medidas robustas de proteção de dados (EXAME, 2019).

Além dos casos de violações de privacidade e imagem, também surgem questões éticas relacionadas à manipulação de conteúdo e informações online. Um exemplo é o fenômeno das *deepfakes*, onde tecnologias de inteligência artificial são usadas para criar vídeos falsos que aparentam ser autênticos. Esses vídeos podem ser utilizados para difamar, desacreditar ou manipular a opinião pública, colocando em dúvida a veracidade das informações compartilhadas online e minando a confiança na mídia e nas instituições.

Diante de todos os fatos envolvendo violações de dados, privacidade e imagem, a problemática eminente na era atual é a dificuldade de identificação de autoria nos casos de violação de imagem causados através da IA, visto que as ferramentas de rastreamento e localização de IP's iniciais não se mostram tão eficazes quando se trata de rastrear a origem da utilização de uma IA. Esse fator ocasiona uma série de empecilhos, sobretudo a segurança de privacidade e justiça para aqueles que tenham seu direito fundamental violado. Sobre tal problemática, Ryan Abbot afirma:

> Poderíamos imaginar que isso criaria uma série de problemas: a primeira pessoa a reconhecer um resultado patenteável pode ser um estagiário em uma grande corporação de pesquisa ou um visitante na casa de alguém. Um grande número de indivíduos também poderá reconhecer simultaneamente um resultado se o acesso a uma IA for generalizado (2016, pg. 1104).

Sendo assim, a distribuição das IA's sem limitações certamente gerará violações de direitos de maneira desenfreada, o que torna necessário que meios de prevenção e combate a

essas violações sejam criados o quanto antes. Em suma, os exemplos e casos práticos mencionados evidenciam a complexidade e urgência da questão da tutela da imagem e privacidade no espaço digital. Essas situações ilustram os riscos e consequências das violações de privacidade e destacam a necessidade de políticas, regulamentações e práticas que garantam uma proteção eficaz dos direitos fundamentais dos indivíduos no ambiente digital.

Contudo, resta evidente a necessidade da criação de ferramentas e métodos de prevenção e proteção da imagem e privacidade dos indivíduos, pois proteger a imagem e a privacidade no espaço digital é crucial na era da tecnologia, onde a disseminação rápida e ampla de informações pode ocorrer sem controle. Com base nos Direitos Humanos, algumas medidas de proteção e prevenção podem ser tomadas e aplicadas.

Sobre a legislação de proteção de dados, mostra-se importante implementar e fortalecer leis de proteção de dados pessoais que regulem a coleta, armazenamento e uso de informações pessoais. Nos últimos anos, houve um aumento significativo na conscientização sobre a importância da proteção de dados pessoais, impulsionado pelo rápido avanço da tecnologia e pela proliferação de serviços digitais. Como resposta a essas preocupações, muitos países têm promulgado legislações específicas para regular o tratamento de dados pessoais por parte de empresas e organizações, uma vez que a legislação de proteção de dados já não é uma opção, mas sim uma necessidade, tendo em vista que a IA veio para ficar, e está crescendo cada vez mais, além de se tornar mais acessível aos indivíduos (FERRAZ, 2021). Um exemplo proeminente é o Regulamento Geral de Proteção de Dados (GDPR), implementado pela União Europeia em maio de 2018. Onde seus principais elementos são:

Consentimento Informado: O GDPR exige que as organizações obtenham o consentimento explícito dos indivíduos para coletar, processar e armazenar seus dados pessoais. Esse consentimento deve ser voluntário, específico, informado e inequívoco (IUBENDA, s.d.).

Direitos dos Titulares dos Dados: O regulamento concede aos titulares dos dados uma série de direitos, incluindo o direito de acessar seus dados, corrigi-los, apagá-los ("direito de ser esquecido"), restringir seu processamento e transferi-los para outra organização (ZOHO, 2019).

Responsabilidade e Prestação de Contas: As organizações são responsáveis por garantir que os dados pessoais sejam processados de maneira legal, justa e transparente. Elas devem

implementar medidas técnicas e organizacionais adequadas para proteger os dados e demonstrar conformidade com o GDPR (SILVA, 2022).

Notificação de Violações de Dados: As organizações são obrigadas a notificar as autoridades de proteção de dados e os titulares dos dados em caso de violações de segurança que possam resultar em riscos para os direitos e liberdades das pessoas afetadas (ZOHO, 2019).

Transferência Internacional de Dados: O GDPR estabelece regras específicas para a transferência de dados pessoais para países fora do Espaço Econômico Europeu, garantindo que essas transferências sejam feitas de maneira segura e legal (ZOHO, 2019).

Impacto Global: Embora o GDPR seja uma legislação europeia, seu impacto é global, pois muitas empresas ao redor do mundo precisam cumprir seus requisitos para fazer negócios com cidadãos europeus. Além disso, ele inspirou a adoção de leis de proteção de dados em outros países e regiões, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e a Lei de Proteção de Dados Pessoais (PDPA) na Índia (GET PRIVACY, s.d.).

Benefícios e Desafios: O GDPR e outras leis de proteção de dados oferecem benefícios significativos para os indivíduos, garantindo maior controle sobre seus dados pessoais e fortalecendo sua privacidade online. No entanto, também apresentam desafios para as organizações, que precisam investir em conformidade, segurança cibernética e governança de dados para evitar multas pesadas e danos à reputação (PORTTUS, 2019).

Em resumo, a legislação de proteção de dados, como o GDPR, desempenha um papel fundamental na promoção da privacidade e da segurança dos dados no espaço digital, garantindo que os direitos humanos sejam respeitados em um contexto cada vez mais orientado pela tecnologia.

Outro método que se mostra interessante é a educação digital, que desempenha um papel crucial na proteção da imagem e da privacidade no espaço digital, capacitando os indivíduos a compreenderem os riscos associados ao uso da tecnologia e a adotarem práticas seguras online. E dentro de seus aspectos importantes, estão:

Conscientização sobre Privacidade: Os programas de educação digital devem incluir informações sobre privacidade online desde as idades mais jovens. Os alunos devem aprender sobre a importância de proteger suas informações pessoais e como fazê-lo (PRIVACY TOOLS, s.d.).

Boas Práticas de Segurança Cibernética: As crianças e jovens devem ser educados sobre boas práticas de segurança cibernética, incluindo a criação de senhas seguras, a identificação de tentativas de *phishing* (cópias falsas de sites reais conhecidos e confiáveis) e a instalação de *software* antivírus. Devem ser incentivados a questionar a autenticidade de fontes de informação online e a verificar a veracidade das informações antes de compartilhá-las (NET CONSULTING, 2023).

Compreensão das Configurações de Privacidade: Os alunos devem aprender a utilizar as configurações de privacidade em redes sociais e outros serviços online para controlar quem pode acessar suas informações pessoais e como suas atividades são rastreadas (NET CONSULTING, 2023).

Respeito aos Direitos Autorais e Propriedade Intelectual: A educação digital deve incluir informações sobre direitos autorais e propriedade intelectual, ensinando os alunos a respeitarem o trabalho criativo de outras pessoas e a não infringir direitos autorais. Conforme destaca o professor Marcos Wachowicz, em palestra online fornecida ao YouTube, afirma que existem quatro principais alternativas consideradas inicialmente para a salvaguarda ou não das produções originadas da inteligência artificial: os trabalhos gerados pela inteligência artificial estariam automaticamente sob domínio público; a posse das criações produzidas pela inteligência artificial pertenceria à empresa que concebeu o aplicativo ou a tecnologia; a posse seria do utilizador; surge a exigência de um novo direito correlato aos direitos autorais para respaldar o direito à empresa que detém tal tecnologia (*Estágio profa Platt UEL*, 2020).

Identificação e Prevenção de Cyberbullying: Os programas de educação digital devem abordar o tema do cyberbullying, ensinando os alunos a reconhecerem comportamentos prejudiciais e a como buscar ajuda se forem vítimas ou testemunhas de cyberbullying (POLIEDRO, 2021).

Desenvolvimento de Pensamento Crítico: Os alunos devem ser incentivados a desenvolver habilidades de pensamento crítico para avaliar informações online, questionar fontes e discernir entre informações confiáveis e enganosas (*Colégio Lindezir Batista*, s.d.).

A educação digital não se trata apenas de alertar sobre os perigos online, mas também de capacitar os alunos a aproveitarem ao máximo as oportunidades oferecidas pela tecnologia de forma segura e responsável.

E como esse método seria implementado? A implementação se daria através de uma série de etapas:

Currículo Escolar: Os princípios de educação digital podem ser integrados ao currículo escolar, abordando temas relacionados à privacidade, segurança cibernética e ética digital em várias disciplinas (GOV, 2024).

Programas de Conscientização: As escolas podem realizar programas de conscientização sobre segurança online, convidando especialistas em segurança cibernética para fornecer palestras e *workshops* para alunos, pais e professores (SERGIO, 2024).

Recursos Online: Existem muitos recursos educacionais online disponíveis, incluindo vídeos, jogos e materiais didáticos, que podem ser utilizados para complementar o ensino presencial sobre educação digital (EDUCACIONAL, 2023).

Parcerias com a Comunidade: As escolas podem estabelecer parcerias com organizações da comunidade, como bibliotecas, centros comunitários e empresas de tecnologia, para oferecer programas de educação digital fora do ambiente escolar (JUSBRASIL, 2016).

Envolvimento dos Pais: Os pais também desempenham um papel importante na educação digital de seus filhos, e as escolas podem fornecer recursos e orientações para ajudá-los a proteger seus filhos online (JUSBRASIL, 2016).

Ante o exposto, a educação digital é essencial para capacitar os indivíduos a protegerem sua imagem e privacidade no espaço digital, promovendo o uso seguro, ético e responsável da tecnologia desde as idades mais jovens. Não obstante, as notificações de violação de dados também serão úteis no que tange à Tutela da Imagem e Privacidade, pois é um componente essencial das leis de proteção de dados. E sobre o processo de aplicação desse método, seus principais aspectos são:

Definição de Violação de Dados: Uma violação de dados ocorre quando há um acesso não autorizado, divulgação, alteração ou destruição de informações pessoais. Isso pode incluir incidentes como vazamento de dados, ataques cibernéticos, perda de dispositivos contendo informações sensíveis, entre outros (MICROSOFT, s.d.).

Obrigação de Notificação: As organizações são obrigadas por lei a notificar as autoridades de proteção de dados e os titulares dos dados afetados em caso de violação de dados

que represente um risco para os direitos e liberdades das pessoas envolvidas. Pois como descrito nas Diretrizes sobre a ocorrência de violação de proteção de dados pessoais do Governo Federal de 2018, a Notificação será realizada por qualquer método adequado, seja por escrito, oralmente ou de outro modo, considerando as circunstâncias específicas da Violação, incluindo o dano que os Indivíduos pertinentes possam sofrer como resultado da Quebra das Regulamentações de Proteção de Dados (MICROSOFT, s.d.).

Conteúdo da Notificação: A notificação de uma violação de dados deve incluir informações específicas, como a natureza da violação, as categorias de dados pessoais afetados, as medidas tomadas para mitigar os efeitos da violação e informações de contato para obter mais detalhes (SECURITY REPORT, 2018).

Prazos de Notificação: O GDPR estabelece prazos específicos para a notificação de violações de dados. As autoridades de proteção de dados devem ser notificadas dentro de 72 horas após a organização ter conhecimento da violação, a menos que a violação não represente um alto risco para os direitos e liberdades das pessoas afetadas (ZOHO, 2019).

Exceções à Notificação: Existem algumas exceções à obrigação de notificação, por exemplo, se a violação de dados for improvável de resultar em um risco para os direitos e liberdades das pessoas afetadas, ou se medidas técnicas e organizacionais adequadas tiverem sido implementadas para proteger os dados (SECURITY REPORT, 2018).

Consequências da Falta de Notificação: A falta de notificação de uma violação de dados pode resultar em penalidades significativas, incluindo multas administrativas impostas pelas autoridades de proteção de dados, além de danos à reputação e à confiança do público na organização afetada (SENADO, 2021).

Ações Pós-Notificação: Após a notificação de uma violação de dados, as autoridades de proteção de dados podem conduzir investigações para avaliar a gravidade da violação e garantir que as medidas corretivas adequadas sejam tomadas pela organização afetada (MICROSOFT, s.d.).

Já no ambiente das redes sociais, um método de proteção da imagem e privacidade é a Criptografia Forte, que é uma técnica fundamental para proteger a privacidade e a segurança das comunicações e dos dados no espaço digital. A criptografia forte refere-se ao uso de algoritmos robustos e métodos eficazes para garantir que as informações permaneçam confidenciais e protegidas contra acessos não autorizados. Os pontos-chave deste método são:

Princípios Básicos da Criptografia: A criptografia envolve a conversão de dados em um formato ilegível, chamado de "texto cifrado", por meio de algoritmos matemáticos complexos. Esse texto cifrado só pode ser decifrado e lido por pessoas ou sistemas autorizados que possuam a chave de criptografia correta (KASPERSKY, 2020).

Algoritmos de Criptografia: Existem vários algoritmos de criptografia disponíveis, cada um com seus próprios métodos e níveis de segurança. Alguns dos mais comuns incluem o algoritmo AES (*Advanced Encryption Standard*), RSA (*Rivest-Shamir-Adleman*), e ECC (*Elliptic Curve Cryptography*) (FASTERCAPITAL, s.d.).

Chaves de Criptografia: As chaves de criptografia são elementos essenciais para o processo de criptografia. Elas são usadas para cifrar e decifrar os dados e podem ser de dois tipos: chaves simétricas, onde a mesma chave é usada para cifrar e decifrar os dados; e chaves assimétricas, onde pares de chaves são usados, uma pública e uma privada, para operações de criptografia e descriptografia (KASPERSKY, 2020).

Criptografia de Ponta a Ponta: A criptografia de ponta a ponta é uma técnica na qual os dados são cifrados no dispositivo de origem e só são decifrados no dispositivo de destino, sem que possam ser interceptados ou lidos por terceiros no meio do caminho. Isso garante uma camada adicional de segurança e privacidade para comunicações online, como mensagens instantâneas, e-mails e chamadas de voz (KASPERSKY, 2020).

Segurança Cibernética: A criptografia forte desempenha um papel fundamental na segurança cibernética, protegendo dados confidenciais contra acessos não autorizados, ataques de hackers, interceptações de comunicações e roubo de informações (KASPERSKY, 2020).

Conformidade com Regulamentações: Em muitos setores, o uso de criptografia forte é exigido por regulamentações de proteção de dados e privacidade, como o GDPR na União Europeia e leis de proteção de dados em outros países. As empresas que lidam com informações sensíveis são obrigadas a implementar medidas adequadas de criptografia para garantir a conformidade legal e a proteção dos dados dos usuários (FULL STACK WEEK, 2024).

Desafios da Criptografia: Embora a criptografia seja uma ferramenta poderosa para proteger a privacidade e a segurança dos dados, ela também apresenta desafios, como a necessidade de gerenciar e proteger adequadamente as chaves de criptografia, a escalabilidade para lidar com grandes volumes de dados e o desenvolvimento contínuo de algoritmos e protocolos criptográficos para acompanhar as ameaças em constante evolução (EVAL, 2018).

Em suma, a criptografia forte é essencial para garantir a confidencialidade e a integridade dos dados no espaço digital, protegendo as comunicações e os dados contra acessos não autorizados e garantindo a conformidade com as regulamentações de privacidade e proteção de dados. Por fim, os métodos e ferramentas propostos para proteger a tutela da imagem e privacidade no espaço digital, sob o enfoque dos direitos humanos na era da tecnologia, são essenciais para garantir que os indivíduos possam desfrutar de seus direitos fundamentais em um ambiente cada vez mais digitalizado. Desde a implementação de legislação de proteção de dados até o fomento da educação digital e o fortalecimento da responsabilidade social corporativa, essas medidas são fundamentais para promover a segurança, a privacidade e o respeito aos direitos humanos em nosso mundo interconectado. Com a adoção de uma abordagem abrangente e colaborativa, será possível criar um ambiente digital mais seguro e ético, onde os direitos individuais sejam protegidos e respeitados em todas as circunstâncias.

CONSIDERAÇÕES FINAIS

A tutela da imagem e privacidade no espaço digital, sob o enfoque dos direitos humanos na era da tecnologia, representa um dos desafios mais prementes e complexos da sociedade contemporânea. Em um mundo onde a tecnologia digital permeia praticamente todos os aspectos da vida cotidiana individual, desde as interações sociais até transações financeiras e serviços governamentais, a proteção dos direitos humanos torna-se fundamental para garantir uma coexistência justa, equitativa e respeitosa.

Nesse contexto, a tutela da imagem e privacidade emerge como uma questão central, pois as informações pessoais, antes guardadas em segredo, agora são compartilhadas e armazenadas em uma escala sem precedentes. A revolução digital trouxe consigo uma série de benefícios e oportunidades, mas também levantou sérias preocupações sobre a segurança e privacidade dos dados pessoais.

Os direitos humanos, fundamentais para a dignidade e liberdade de cada indivíduo, devem ser protegidos e respeitados no espaço digital da mesma forma que são no mundo físico. Isso requer a implementação de medidas eficazes para garantir a integridade, confidencialidade e disponibilidade das informações pessoais, bem como para prevenir abusos e violações por parte de indivíduos, empresas e governos.

Uma abordagem holística e multidisciplinar é necessária para enfrentar os desafios da tutela da imagem e privacidade no espaço digital. Isso envolve não apenas a promulgação de

leis e regulamentos robustos de proteção de dados, mas também o desenvolvimento de tecnologias e práticas que garantam a segurança e privacidade dos usuários.

A educação digital desempenha um papel crucial nesse processo, capacitando os indivíduos a compreenderem os riscos e desafios associados ao uso da tecnologia, bem como a adotarem práticas seguras e responsáveis online. A conscientização sobre os direitos humanos, incluindo o direito à privacidade e à proteção de dados, é essencial para promover uma cultura de respeito e responsabilidade no espaço digital.

Além disso, a colaboração entre diferentes partes interessadas, incluindo governos, empresas, organizações da sociedade civil e a comunidade acadêmica, é fundamental para abordar os complexos problemas relacionados à tutela da imagem e privacidade no espaço digital. Somente através de esforços conjuntos e coordenados será possível desenvolver soluções eficazes e sustentáveis para proteger os direitos humanos na era digital.

A responsabilidade social corporativa desempenha um papel importante nesse contexto, incentivando as empresas a adotarem práticas éticas e transparentes em relação à coleta, armazenamento e uso de informações pessoais. As empresas têm a responsabilidade de garantir que os direitos dos usuários sejam respeitados e protegidos em todas as suas operações, contribuindo assim para a construção de um ambiente digital mais seguro e confiável para todos.

Por fim, é crucial lembrar que a tutela da imagem e privacidade no espaço digital não é apenas uma questão técnica ou jurídica, mas também uma questão de valores e princípios fundamentais. Na era da tecnologia, é mais importante do que nunca defender os direitos humanos como um imperativo moral e legal, garantindo que todos os indivíduos possam desfrutar de sua liberdade, dignidade e privacidade em um mundo cada vez mais interconectado.

REFERÊNCIAS

A IMPORTÂNCIA DA EDUCAÇÃO EM SEGURANÇA CIBERNÉTICA. Net Consulting. Sd. Disponível em: https://netconsulting.com.br/a-importancia-da-educacao-em-seguranca-cibernetica/#:~:text=Boas%20Pr%C3%A1ticas%20de%20Seguran%C3%A7a&text=Isso%20

inclui%20a%20cria%C3%A7%C3%A3o%20e,backup%20regularmente%20de%20dados%20importantes. Acesso em 14 abr. 2024.

A IMPORTÂNCIA DO PENSAMENTO CRÍTICO NA ERA DA INFORMAÇÃO. Colégio Lindezir Batista. Sd. Disponível em: https://colegioclb.com.br/noticias/aimportanciadopensamentocritico/#:~:text=O%20pensamento%20cr%C3%ADtico%20%C3%A9%20uma,formar%20opini%C3%B5es%20embasadas%20em%20evid%C3%AAncias. Acesso em 09 mai. 2024.

ABBOTT, Ryan. I Think, Therefore I invent: Creative Computers and the Future of Patent Law. Vol. 57. Boston: Boston College Law Review, 2016.

ADRIANO, Leila. Direitos Autorais no Ensino a Distância: Guia Completo para Utilização Responsável de Conteúdo. Ago. 2023. Disponível em: https://www.digitalsemmisterios.com/blog/direitos-autorais-no-ead. Acesso em: 14 abr. 2024.

AES, RSA, ECC E MUITO MAIS. Faster Capital Sd. Disponível em: https://fastercapital.com/pt/tema/aes,rsa,eccemuitomais.html#:~:text=O%20ECC%20%C3%A9%20mais%20eficiente,digitais%20e%20troca%20de%20chaves. Acesso em 05 out. 2024.

ANDRADE, Geraldo. Direito à Privacidade: intimidade, vida privada e imagem. Disponível em: https://www.jusbrasil.com.br/artigos/direito-a-privacidade-intimidade-vida-privada-e-imagem/214374415#:~:text=A%20Constitui%C3%A7%C3%A3o%20Federal%20no%20art,moral%20decorrente%20de%20sua%20viola%C3%A7%C3%A3o. Acesso em 04 mai. 2024.

ARAÚJO, Janaína. Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos. RádioSenado. Mar. 2023. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dezanosdevigenciadaleicarolinadieckmannaprimeiraapunircrimescibernеticos#:~:text=A%20Lei%2012.737%2F2012%2C%20conhecida,sofrer%20uma%20tentativa%20de%20extors%C3%A3o.

AYUSO, Rocío. Lawrence: “Não é um escândalo, é um crime sexual”. Estilo. Out. 2014. Disponível em: https://brasil.elpais.com/brasil/2014/10/07/estilo/1412701030_253903.html. Acesso em 05 Mar. 2024.

BBC NEWS. Entenda o escândalo de uso político de dados que derrubou valor do Facebook r o colocou na mira de autoridades. Globo. Mar. 2024. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalodeusopoliticodedados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em set. 2024.

BOSCIONI, Gabriel. Dimensões dos Direitos Humanos. Estratégia. Jun. 2023. Disponível em: https://www.estrategiaconcursos.com.br/blog/dimensoes-dosdireitos-humanos/. Acesso em 12 jun. 2024.

BRASIL. Câmara dos Deputados. João Arruda - PMDB/PR. PL 5555/2013. Altera a Lei nº 11.340, de 7 de agosto de 2006 - Lei Maria da Penha - criando mecanismos para o combate a condutas ofensivas contra a mulher na Internet ou em outros meios de propagação da informação. Portal da Câmara dos Deputados: Brasília, DF, p. 1, 2013.

BRASIL. Câmara dos Deputados. Romário - PSB-RJ. PL 6630/2013. Acrescenta artigo ao Código Penal, tipificando a conduta de divulgar fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima e dá outras providências. Portal da Câmara dos Deputados: Brasília, DF, p. 1, 2013.

CAROLINA, Ellen. Autorregulação regulada: instrumento de prestação de contas com a LGPD. Consultor Jurídico. Dez. 2022. Disponível em: https://www.conjur.com.br/2022-dez-16/ellen-silva-prestacao-contas-lgpd/. Acesso em 12 abr. 2024.

CONHEÇA 6 RECURSOS EDUCACIONAIS DIGITAIS PARA USAR NA SUA ESCOLA. Educacional. Sd. Mai. 2023. Disponível em: https://educacional.com.br/tecnologiaeducacional/recursoseducacionaisdigitais/#:~:text=Videoaulas%2C%20question%C3%A1rios%20online%2C%20games%2C,exemplos%20de%20recursos%20educacionais%20digitais.&text=Um%20dos%20objetivos%20do%20Programa,nas%20redes%20de%20educa%C3%A7%C3%A3o%20b%C3%A1sica. Acesso em 11 ago. 2024.

CYBERBULLYNG: ELABORA JUNTO COM A ESCOLA FORMAS DE CONSCIENTIZAÇÃO E PREVENÇÃO. Poliedro. Sd. Dez. 2021. Disponível em: https://www.colegiopoliedro.com.br/blog/cyberbullying-elabore-junto-com-a-escola-formas-de-conscientizacao-e-prevencao/. Acesso em 08 mai. 2024.

DEFINIÇÃO DE VIOLAÇÃO DE DADOS. Microsoft. Sd. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-a-data-breach. Acesso em 11 ago. 2024.

EDUCAÇÃO EM PRIVACIDADE DIGITAL E A IMPORTÂNCIA DE PROTEGER A IDENTIDADE DOS CLIENTE. Privacy tools. Sd. Disponível em: https://www.privacytools.com.br/educacao-em-privacidade-e-a-protecao-da-identidade-dos-clientes/. Acesso em 13 abr. 2024.

ELIAS, Raquel *et al.* Direitos Humanos Fundamentais. 2019. Disponível em: https://www.mpf.mp.br/pgr/documentos/coletanea_direitos_humanos_fundamentais.pdf. Por Ministério Público Federal.

EMERJ. Inteligência Artificial e Direito à Privacidade – Carlos Affonso Souza. Jul. 2019. Disponível em: https://www.youtube.com/watch?v=rTY3SB0LO_k&t=331s&ab_channel=EMERJ. Acesso em 04 out. 2024.

ESTÁGIO PROFA. PLATT UEL 2020. Formação para Trabalhadores da Educação Pública do PARANÁ/APP/UEL 2020: DIREITOS AUTORAIS. Disponível em: https://www.youtube.com/watch?v=YwsuVOwJM4U&ab_channel=Est%C3%A1gioprofa.PlattUEL2020. Acesso em 08 mai., 2024.

EXAME. Equifax pagará até US$ 700 milhões por vazamento de dados pessoais. Jul. 2019. Disponível em: https://exame.com/negocios/equifax-pagara-ate-us-700-milhoes-por-vazamento-de-dados-pessoais/. Acesso em 05 Mar. 2024.

FERRAZ, Paula *et al*. A importância da conscientização sobre a proteção dos dados pessoais. Consultor Jurídico. Out. 2021. Disponível em: https://www.conjur.com.br/2021-out-02/opiniao-conscientizacao-protecao-dados-pessoais/. Acesso em 05 out. 2024.

FLORIDI, Luciano. A inteligência artificial está reconstruindo o mundo. Instituto Humanitas Unisinos. Entrevista concedida a Diego de Angelis. "A inteligência artificial está reconstruindo o mundo". Entrevista com Luciano Floridi, dezembro/2021.

FRANCIULLI, Domingos. A proteção ao Direito à Imagem e a Constituição Federal. Biblioteca Ministro Oscar Saraiva. Vol. 16, n° 1. Jan/jul 2004. Disponível em: file:///C:/Users/thiag/Downloads/442-1637-1-PB.pdf. Acesso em 04 mai. 2024.

IUBENDA. Exemplos de formulário de consentimento no GDPR – O que fazer ou evitar. Sd. Disponível em: https://www.iubenda.com/pt-br/help/78933-exemplos-de-formulario-de-consentimentonogdproquefazerouevitar#:~:text=O%20GDPR%20exige%20que%20as,e%20envolver%20uma%20a%C3%A2a. Acesso em 12 abr. 2024.

LGPD e GDPR: ENTENDA A DIFERENÇA E SEMELHANÇA ENTRE AS LEIS. Sd. Get Privacy. Disponível em: https://getprivacy.com.br/lgpd-gdpr-diferencas-semelhancas/#:~:text=A%20LGPD%20. Acesso em 13 abr. 2024.

LUIZA, Anna *et al*. Era uma vez em Bollywood: nova lei de proteção de dados pessoais da Índia. Consultor Jurídico. Nov. 2023. Disponível em: https://www.conjur.com.br/2023-nov-26/era-uma-vez-em-bollywood-nova-lei-de-protecao-de-dados-pessoais-da-india/. Acesso em 06 mai. 2024.

MARINHO, Juliana. Cyberbulling: A exposição indevida e seus impactos no caso Amanda Todd. Jusbrasil. 2019. Disponível em: https://www.jusbrasil.com.br/artigos/cyberbullying-a-exposicao-indevida-e-seus-impactos-no-caso-amanda-todd/746037224. Acesso em 05 Mar. 2024.

MARTINS, Américo. Eleições nos EUA: uso de deepfake e IA revela problema que pode se repetir no Brasil. CNN Brasil. jan. 2024. Disponível em: https://www.cnnbrasil.com.br/internacional/eleicoes-nos-eua-uso-de-deepfake-e-ia-revela-problema-que-pode-se-repetir-no-brasil/. Acesso em set. 2024.

MEC DISCUTE EDUCAÇÃO DIGITAL E CURRÍCULO. Gov. Abr. 2024. Disponível em: https://www.gov.br/mec/pt-br/assuntos/noticias/2024/abril/mec-discute-educacao-digital-e-curriculo. Acesso em 10 ago. 2024.

MORAES, Alexandre. Direito Constitucional: 13° edição atualizada com a EC n° 39/02. Disponível em: https://jornalistaslivres.org/wp-content/uploads/2017/02/DIREITO_CONSTITUCIONAL-1.pdf. Acesso em 06 mai. 2024.

NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos. Nova Iorque: ONU, 1948. Disponível em: https://www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese?LangID=por. Acesso em 15 ago. 2024.

O QUE É CRIPTOGRAFIA DE DADOS? DEFINIÇÃO E EXPLICAÇÃO. Kaspersky. Sd. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/encryption. Acesso em 04 out. 2024.

PIOVESAN, Flávia. Direitos Humanos: Desafios e Perspectivas Contemporâneas. TST, Brasília. Vol. 75. 2009. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/6566/010_piovesan.pdf.

PROTEÇÃO DE DADOS PESSOAIS – SEUS DESAFIOS E BENEFÍCIOS. Porttus. Mai. 2019. Disponível em: https://porttus.com/protecao-de-dados-pessoais-seus-desafios-e-beneficios/. Acesso em 13 abr. 2024.

SANTOS, Jeverson. Importância da Criptografia de arquivos: Normas e Melhores Práticas. Full Stack Week. Mai. 2024. Disponível em: https://www.dio.me/articles/importancia-da-criptografia-de-arquivos-normas-e-melhores-praticas. Acesso em 05 out. 2024.

SENADO, Agência. Punições pelo uso indevido de dados pessoais começam a valer no domingo. Senado Notícias. Jul. 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/07/29/punicoes-pelo-uso-indevido-de-dados-pessoais-comecam-a-valer-no-domingo. Acesso em 03 out. 2024.

SERGIO MARTINS, Paulo. Programa Municipal de EDUCAÇÃO DIGITAL em atendimento ao disposto na LF n° 14.811/2024. Câmara Municipal de Jundiaí/SP. 2024. Disponível em: https://sapl.jundiai.sp.leg.br/sapl_documentos/proposicao/64389_signed.pdf. Acesso em 10 ago. 2024.

SLM ADVOGADOS. Educação Digital e a parceria entre a escola e a família. Jusbrasil. 2016. Disponível em: https://www.jusbrasil.com.br/artigos/educacao-digital-e-a-parceria-entre-a-escola-e-a-familia/438998205. Acesso em 11 ago. 2024.

SOFTWARE DE CRIPTOGRAFIA: BENEFÍCIOS E DESAFIOS. Sd. Ago. 2018. Disponível em: https://eval.digital/blog/protecao-de-dados/software-de-criptografia-beneficios-e-desafios/. Acesso em 05 out. 2024.

TRABALLI, Arthur. A inviolabilidade à intimidade, à vida privada, à honra, à imagem: dano material, moral ou à imagem. Jusbrasil. 2016. Disponível em: https://www.jusbrasil.com.br/artigos/a-inviolabilidade-a-intimidade-a-vida-privada-a-honra-a-imagem-dano-material-moral-ou-a-imagem/337428559. Acesso em 12 jun. 2024.

VÍDEOS FALSOS E DEEPFAKE – COMO OS USUÁRIOS PODEM SE PROTEGER. Kaspersky. Disponível em: https://www.kaspersky.com.br/resource-center/threats/protect-yourself-from-deep-fake. Acesso em 05 Mar. 2024.

VIOLAÇÕES DE DADOS E GDPR: O QUE VOCÊ PRECISA SABER. Security Report. Sd. Disponível em: https://securityleaders.com.br/violacoesdedadose/#:~:text=Nos%20termos%20do%20artigo%2033,de%20registros%20de%20dados%20pessoais. Acesso em 03 out. 2024.