AI, DATA PRIVACY, AND THE RIGHT TO BE FORGOTTEN: NAVIGATING HUMAN RIGHTS IN THE AGE OF GENERATIVE TECHNOLOGY

Divya Hariharan, LL.M., Khwaja Moinuddin Chishti Language University, Lucknow

Harsh Kumar Singh, LL.M., Khwaja Moinuddin Chishti Language University, Lucknow

ABSTRACT

The rapid growth of generative AI technologies has raised significant questions about data privacy, authorship, and individual rights. With AI-generated content becoming ubiquitous, concerns surrounding the "Right to be Forgotten" have gained prominence, especially about how personal data is used, transformed, and stored by AI systems. This paper explores how generative AI intersects with human rights law, particularly focusing on data rights and privacy protection. The primary research question is: How do generative AI systems infringe upon individual data rights, and how can existing legal frameworks be adapted to safeguard these rights?

The paper's objective is to examine the adequacy of current national and international data protection laws, with particular emphasis on India's Digital Personal Data Protection Act, 2023, and the European Union's GDPR. Through doctrinal legal research, the paper evaluates the legal and ethical challenges arising from AI-driven data collection, consent, and transparency. It identifies key gaps in the regulatory frameworks and the need for clearer legal safeguards, particularly regarding consent and algorithmic transparency.

The paper concludes by advocating for a rights-based approach to AI regulation that incorporates the Right to be Forgotten and stronger legal protections to ensure that the development of AI technologies aligns with fundamental privacy rights and human dignity in the digital age.

Keywords: Generative AI, Right to be Forgotten, Data Privacy, Legal Frameworks, Artificial Intelligence Regulation.

I. Introduction

In recent years, generative artificial intelligence (AI) has become a powerful force in the digital world. Technologies like text-to-image generators, deepfake software, AI music creators, and chatbots are changing the way we create, communicate, and express ourselves. These tools can produce highly realistic images, mimic artistic styles, compose music, and generate text, often with little human input. One of the most popular examples of this technology is AI-generated portraits in the style of Studio Ghibli, which have become viral on social media platforms.

While these innovations offer exciting new opportunities for creativity and accessibility, they also raise important legal and ethical issues that haven't been fully addressed. The main concern is that the excitement around AI-generated creativity often overlooks the hidden costs to privacy, consent, and data protection.

Generative AI models are typically trained using large datasets scraped from the internet, including personal images, social media content, and user-generated materials, often without the consent of the individuals whose data is used. This means every day, people may become involuntary contributors to AI training data, exposing them to risks like identity theft, unauthorized use of their data, and long-term digital profiling. While the outputs created by AI might seem original, they are often based on the personal, cultural, and creative work of real individuals, raising concerns of exploitation and loss of control over one's digital identity.

One of the biggest issues with these AI systems is their lack of transparency. When users upload personal data, like a selfie for transformation, they often have no idea where their data is going, how long it will be stored, or if it will be used again. Terms of service are often vague, consent is hidden under complex legal language, and there is little to no possibility for users to delete or withdraw their data once it's been used. This situation makes concepts like informed consent and data minimization, which are key principles of modern data protection laws, almost meaningless.

This article will explore the intersection of generative AI and human rights, focusing on the right to privacy and the emerging right to be forgotten. These rights, protected by international law and India's constitutional framework, are increasingly challenged by the rise of AI technologies. While India has made progress with the introduction of the Digital Personal Data

Protection Act, 2023 (DPDPA), the law does not fully address the unique risks posed by generative AI, including deepfakes, digital identity replication, and algorithmic data retention.

By comparing India's legal framework to global data protection standards like the EU's General Data Protection Regulation (GDPR) and the AI governance principles outlined by UNESCO and the OECD, this article argues that current safeguards are not enough to deal with the new digital threats. As AI becomes more embedded in our lives, it is urgent to rethink consent, data rights, and privacy in a way that prioritizes dignity, autonomy, and human-centered technology.

The goal is not to stop innovation but to ensure that these technologies, which have the potential to empower creativity, do not undermine the very rights that make creativity meaningful. The future of AI should not only be intelligent and efficient but also just, inclusive, and respectful of human rights.

II. Generative AI and the Data Dilemma: Opportunities and Risks

Generative Artificial Intelligence (AI) represents one of the most transformative technological innovations of our time. At its core, generative AI refers to a class of machine learning models capable of creating novel outputs, whether images, text, audio, or video, by identifying and mimicking patterns from large training datasets. Prominent tools like OpenAI's DALL·E, Midjourney, and Stability AI's Stable Diffusion exemplify this capability, producing aesthetically compelling content that often blurs the line between machine output and human creativity.

However, these models work by using huge amounts of data, much of which is collected randomly from the internet. These datasets frequently include personal photographs, social media content, copyrighted artworks, and culturally specific symbols, often acquired without the informed consent of the creators or subjects. This raises urgent legal and ethical questions around data ownership, privacy, and accountability.

A prominent example is the growing popularity of AI-generated portraits styled after well-known animation studios, such as Studio Ghibli or Pixar. Users are encouraged to upload selfies to see themselves reimagined in fun, stylized forms, which seems harmless but hides a bigger issue. Once images are uploaded, users often lose control over their data and unknowingly contribute to the ongoing training of the model. There's no guarantee that the images will be deleted, and it's unclear how they may be stored, reused, or even sold.

This loss of control over personal data becomes particularly problematic in the absence of robust legal frameworks. Most platforms' terms of service are dense, technical, and designed to obscure rather than clarify. They often include blanket licenses that allow companies to reproduce, modify, and share user data, with little or no options for redress. In effect, users become data contributors to a system with no compensation, recognition, or ability to withdraw consent. The lack of a clear process for data deletion or the Right to be Forgotten is even more concerning as AI-generated content spreads.

Further complicating the landscape is the phenomenon of artistic appropriation. Generative AI models are increasingly capable of replicating the distinctive visual styles of living artists, leading to a contentious debate about authorship, attribution, and copyright. While current copyright laws are designed to protect fixed expressions of ideas, they are ill-equipped to handle the stylized mimicry produced by machine learning algorithms. Artists have raised concerns that their life's work is being commodified without consent, especially when AI-generated content is sold on commercial platforms, eroding both economic rights and creative identity.

Perhaps the most troubling dimension is the potential misuse of personal data through generative models. AI systems trained on scraped images can produce new outputs that resemble real individuals, including features, poses, and even emotional expressions. This has given rise to **deepfakes**, wherein individuals are placed in fabricated videos or images, often in compromising or defamatory contexts. In extreme cases, these technologies have been weaponized for harassment, identity theft, or political misinformation, with little recourse available to victims.

Moreover, because generative AI systems learn from patterns, they can create new content that closely mimics a person's appearance, style, or speech, even if that person never directly contributed to the training data. This creates a troubling possibility of involuntary digital replication, where a person's likeness is not only stored but actively recreated by machines. Yet, there is no clear legal obligation for companies to inform users, seek explicit consent, or allow the deletion of this inferred data. This lack of clear mechanisms for data deletion highlights the urgent need for laws to address the Right to be forgotten in the context of generative AI.

This growing gap between AI innovation and data accountability points to a dangerous trend. It creates an environment where convenience is prioritized over consent, creativity overrides rights, and technological progress moves faster than regulatory control. Individuals, often attracted by the novelty and ease of generative tools, are turned into involuntary participants in a hidden and exploitative data economy.

In this situation, the lack of enforceable legal rights and clear ethical standards exposes users to long-term data exploitation, reputational harm, and psychological risks. Without strong regulations, such as AI-specific privacy laws, data transparency requirements, and algorithmic accountability measures, the generative AI landscape risks becoming a digital Wild West where rights are unclear and abuses are accepted. Legal frameworks must change to address these risks and ensure that individuals have the Right to be forgotten—to withdraw, delete, and control their data after it has been used by AI systems.

India, like many other countries, is at a turning point. The Digital Personal Data Protection Act, 2023, is a good start toward protecting user data, but it doesn’t fully address the new risks created by generative AI. Without clear rules, people continue to share their personal data for fun or convenience, not realizing that this data is used by systems that are complex, unclear, and difficult to understand.

As generative AI changes the way we create content and express ourselves online, our laws and policies must also change. They need to focus more on openness, consent, and giving users control over their data. Only then can we make sure that technology supports human dignity and respects democratic values.

III. The Right to Privacy and the Right to be Forgotten: Evolving Human Rights in the Digital Age

The right to privacy is a fundamental aspect of human dignity, autonomy, and freedom. It protects an individual's personal space, including their thoughts, communications, and identity, from unwarranted interference by the state, corporations, or private entities. Globally, this right is recognized as a universal human right and is protected under Article 12 of the Universal

Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. These international frameworks emphasize every individual's right to be free from arbitrary or unlawful intrusions into their personal life, family, home, or correspondence.

In today's digital environment, the meaning of privacy has changed significantly. Privacy is no longer limited to physical spaces; it now includes online activity, digital behaviour, and the data people unknowingly generate. Metadata, browsing history, behavioural patterns, and predictions about individuals all form part of this expanded notion of digital privacy. As data becomes central to identity, individuals are increasingly tracked, analysed, and categorized by advanced technologies, often without their knowledge or consent.

Alongside the right to privacy is the growing importance of the right to be forgotten. This right allows individuals to request the removal of personal data that is outdated, no longer relevant, or collected without valid consent. It was first formally recognized in Article 17 of the European Union's General Data Protection Regulation. This legal provision aims to give people more control over their digital presence. However, enforcing this right becomes particularly challenging in the context of artificial intelligence, especially with generative AI.

Generative AI systems operate very differently from traditional data storage systems. When an AI model is trained on data such as a photo, a voice recording, or a text message, that data is not saved in its original form. Instead, it is absorbed into the system through a process of learning patterns, which are then used to produce future outputs. This makes it extremely difficult to remove specific data once it has been used. In many cases, completely removing the influence of that data would require retraining the entire model, which is technically complex, costly, and not currently required under most laws.

In India, the right to privacy was recognized as a constitutional fundamental right through the Supreme Court's landmark decision in *Justice K.S. Puttaswamy v. Union of India* in 2017. The Court held that privacy is an essential part of the right to life and personal liberty under Article 21 of the Constitution. It highlighted the importance of consent, informational self-determination, and data protection in the digital era. Despite this judicial progress, there is still no clear legislation in India addressing the right to be forgotten, and how it applies to artificial intelligence remains uncertain.

The use of generative AI makes this gap more concerning. People often share their photos, voices, and personal details on AI platforms, sometimes without fully understanding how this data will be used. These platforms can retain elements such as facial features, voice styles, or emotional tones that continue to influence the system's outputs long after the original data was uploaded. Even if someone requests deletion of their data, the AI might still produce content that resembles or reflects them. This undermines the spirit of the right to be forgotten, especially when such content is used in misleading or harmful ways.

Another serious issue is the ability of AI to infer deeply personal information with very little input. For example, AI systems can use small pieces of data to predict sensitive attributes like political views, religious beliefs, mental health conditions, or sexual orientation. These insights can then be used for advertising, surveillance, or even profiling, often without the person's knowledge. As a result, individuals may face judgment, bias, or harm without ever knowing how or why these assumptions were made.

There is also a growing power imbalance between technology developers and everyday users. Most users are not fully aware of how their data is processed, who has access to it, or how long it is stored. Privacy policies are often written in complex legal language that most people do not read or understand. This leads to a situation where people give away their data rights without realizing it, while companies benefit from the data to create advanced products and services.

In this scenario, protecting privacy and enforcing the right to be forgotten is not just a legal responsibility but a moral one. As AI continues to expand, governments must develop new interpretations of human rights that reflect the realities of modern technology. This includes creating clear and enforceable laws that allow people to request the removal of their data from AI models, ensuring transparency about how data is used, and designing systems that allow users to give and withdraw consent in meaningful ways.

India should consider incorporating the right to be forgotten into its domestic laws as part of a broader approach to AI regulation. This right should be practical, enforceable, and supported by mechanisms that help resolve disputes fairly. Alongside this, there should be investments in making AI systems more transparent, conducting ethical audits, and educating the public so that everyone can make informed decisions about their data.

Without these protections, individuals risk becoming invisible and powerless in a digital world where they are copied, misrepresented, and judged by systems they cannot see or control. Upholding the right to privacy and the right to be forgotten in the age of AI is essential not only for data protection but for safeguarding human dignity itself.

IV. India's Legal Framework: Progress, Challenges, and the Way Forward

A. Progress

India’s digital landscape is expanding rapidly due to greater internet access, increasing innovation, and a growing number of digitally literate citizens. In response to rising concerns over data protection and digital rights, the Digital Personal Data Protection Act, 2023 (DPDPA) marks a significant step forward. It introduces key principles such as informed consent, purpose limitation, and data minimization. The Act grants individuals the right to access, correct, and delete their personal data. It also imposes obligations on data fiduciaries to process information responsibly.

This legislation lays the groundwork for protecting privacy in traditional data ecosystems. It establishes a structure for accountability and gives users a degree of control over their personal information. The formation of the Data Protection Board of India (DPBI) represents an initial move towards enforcement and oversight.

B. Challenges

Despite its strengths, the DPDPA has important limitations, especially in the context of generative artificial intelligence. It does not address the complex ways in which AI systems collect, process, and reuse data. For instance, generative AI models learn from patterns within datasets, embedding information into algorithms rather than storing it in an easily traceable format. This makes it difficult to determine whether and how personal data is being used.

A key issue is the unclear status of anonymized or inferred data. When a user uploads content, such as an image, to an AI platform, the system may extract features or styles that later appear in generated content. Even without storing the original image, the outputs may reflect identifiable traits. The law does not clarify whether such outputs are protected under data privacy rules.

Another major gap is the absence of AI-specific provisions. Unlike jurisdictions such as the

European Union, which apply a risk-based approach under their proposed AI Act, the Indian framework treats all data handlers similarly. This lack of distinction leaves high-risk activities such as deepfakes, automated profiling, and synthetic impersonation unregulated.

The consent model under the DPDPA is also poorly suited for AI systems. Users often accept standard terms without understanding how their data might be used. In AI environments, this can mean unknowingly contributing data for commercial training or content creation. This kind of uninformed and broad consent undermines meaningful user choice and digital autonomy.

Additionally, the enforcement mechanism under the DPBI raises concerns. Its independence, authority, and technical capacity to oversee AI technologies remain uncertain. It does not currently have the power to demand algorithmic transparency, require impact assessments, or conduct audits. Without strong oversight, individuals have limited protection against misuse or algorithmic harm.

C. The Way Forward

India needs a rights-based and forward-looking legal framework to meet the challenges of the AI age. This should include specific legislation on artificial intelligence that addresses unique harms, ensures transparency, and upholds user rights. Clear definitions, risk-based classifications, and legal obligations for developers would help bring accountability to the AI space.

Consent practices must also be reformed to allow more informed, granular, and revocable decisions by users. This is especially important for sensitive data such as facial features, voice recordings, or personal writing used in generative models.

Building strong institutions is equally essential. India should establish independent AI regulators, ethics committees, and public grievance mechanisms to monitor and respond to potential risks. These bodies should have the authority to investigate complaints, enforce rules, and provide remedies for affected individuals.

Finally, the broader goal should be to protect not just personal data, but also digital identity, human dignity, and constitutional freedoms. As AI becomes part of everyday life in India, the legal system must evolve to ensure that innovation does not come at the cost of fundamental rights.

V. Ethical Concerns and the Human Rights Perspective on AI Governance

Generative AI systems raise serious ethical concerns that go beyond legal regulation. These technologies sit at the intersection of creativity, identity, and power, often operating without enough oversight or accountability. As AI becomes a bigger part of daily life, it challenges our traditional ideas of authorship and privacy. It also risks reinforcing social inequalities that already exist. To address these concerns, a human rights approach to AI must go beyond following the law and ask deeper questions about who controls technology, who benefits, and who might be harmed.

One of the main ethical issues is artistic appropriation and cultural mimicry. AI models are trained on large datasets taken from the internet, which often include unique artistic styles. These styles are absorbed without the creator's permission, knowledge, or compensation. For example, AI might imitate the style of well-known studios or individual artists. This raises questions about intellectual property and authorship. Traditional copyright laws are not yet equipped to deal with these issues in the context of AI-generated content.

Another concern is digital consent and user autonomy. People often use AI-powered tools like face filters or art generators without fully understanding how their personal data is used. Many users simply accept long, complex terms of service without reading them, leading to what's known as "consent fatigue." As a result, users lose control over their digital identities. This creates an imbalance, where developers and companies hold most of the power, while users are left unaware that their data might be used to train models that can later reproduce or distort their likeness or voice.

Generative AI systems also have the potential to amplify biases. AI can unintentionally reinforce stereotypes based on the data it has been trained on. For example, an AI image generator might default to using stereotypes when creating images of people from certain racial or gender groups. This is especially harmful to marginalized communities whose identities might be misrepresented or left out. If AI is not guided by ethical principles, it can become an amplifier of social biases rather than a neutral tool.

Moreover, many generative AI systems operate as "black boxes," meaning their decision-making processes are not transparent. When AI generates content or makes decisions, it's often unclear how or why it came to a particular conclusion. This lack of transparency makes it hard for people to question or challenge AI decisions, undermining accountability and due process.

Recognizing these ethical challenges, the international community has begun to stress the importance of ethical and human-centered AI governance. Organizations like UNESCO and the OECD have published guidelines that emphasize the need for transparency, fairness, and accountability in AI systems. These frameworks urge governments and developers to embed human rights principles into the design and development of AI technologies.

For India, adopting a human rights-based approach to AI means addressing these issues through new laws, better institutions, and involvement from all stakeholders. It's essential to create an environment where civil society groups, artists, technologists, legal experts, and policymakers can work together to develop ethical standards that reflect India's diverse culture. India should also focus on creating inclusive AI systems that protect marginalized voices and give them the power to shape AI technologies in the future.

As generative AI becomes a more integral part of various sectors like entertainment, education, and even law enforcement, the ethical questions surrounding its use cannot be ignored. The goal is not just to regulate technology but to ensure that it serves humanity and upholds values like dignity, fairness, and equality.

VI. Recommendations: Bridging Legal, Ethical, and Technological Gaps

To address the widening gap between technological advancements and the protection of human rights, a proactive and rights-centric regulatory approach is necessary. The following recommendations aim to guide policymakers, developers, and civil society toward creating a more ethical and accountable AI ecosystem:

- **Introduce AI-Specific Legislation**: India must enact dedicated laws that address the unique challenges posed by Artificial Intelligence. This includes defining AI systems, ensuring transparency, and establishing legal standards for data used in training generative models. Developers should be required to disclose how personal data is collected, processed, and retained, particularly when used for AI training datasets.
- **Strengthen the Right to Be Forgotten**: Amend the Digital Personal Data Protection Act, 2023, to explicitly apply the right to be forgotten to AI systems. This includes

mechanisms for individuals to request the removal of their data from AI training datasets and to have AI-generated content based on their likeness or personal inputs erased.

- **Mandate Algorithmic Transparency and Audits**: AI platforms should be required to perform regular algorithmic audits and impact assessments, especially for applications involving biometric data, facial recognition, or generative content. These audits should assess risks related to bias, misinformation, and privacy violations, and the results should be made publicly available.

- **Enforce Informed and Ongoing Consent**: Consent should not be limited to a single checkbox. Platforms must provide granular consent options, allowing users to opt in or out of specific data uses. Furthermore, consent should be an ongoing process, with users regularly informed of any changes to data usage policies.

- **Promote Ethical AI by Design**: Developers and tech companies should be encouraged (or required) to adopt ethical design principles that prioritize human rights. This includes mechanisms to prevent discriminatory content, safeguards against deepfakes, and protocols for redress in cases of harm.

- **Foster Digital Literacy and Public Awareness**: The asymmetry of knowledge between users and technology providers is a significant issue. Government agencies, educational institutions, and civil society should collaborate to build digital literacy programs that help individuals understand their rights and risks in the AI-driven digital environment.

- **Encourage Global Collaboration and Alignment**: Given the global nature of AI technologies, India should align its regulatory framework with international standards, such as the GDPR and UNESCO's Recommendation on the Ethics of Artificial Intelligence. Participation in global dialogues on AI governance will ensure that India's approach remains robust and forward-looking.

By implementing these recommendations, India can align innovation with human dignity, ensuring that AI growth does not come at the cost of privacy, autonomy, and fundamental rights.

VII. Conclusion

The rapid growth of generative AI technologies has significantly transformed creativity, communication, and convenience. However, this shift has also brought several legal, ethical, and human rights challenges. From AI-generated art to deepfakes and automated text generation, these technologies are changing how we interact with digital platforms. However, these innovations come at a cost, as individuals often unknowingly trade their personal data, likeness, and digital identity in exchange for access to these tools.

As users continue to upload personal data, such as images, voices, and preferences, into AI systems that run on opaque algorithms and lack strong accountability, core rights like privacy, informed consent, and digital dignity are increasingly at risk. Unlike traditional technologies, generative AI can retain and repurpose user data in abstract and irreversible ways. This raises concerns about the permanence of data and the lack of meaningful control over one's digital presence.

India has made a significant step forward with the Digital Personal Data Protection Act, 2023, but this legislation is only a starting point. While it provides essential procedural rights and acknowledges the importance of data protection, it does not fully address the complexities of AI systems. Challenges such as algorithmic opacity, cultural misappropriation in AI-generated art, and the re-identification of anonymized data remain largely unresolved. Additionally, there is still a lack of legal clarity regarding the enforcement of the right to be forgotten, particularly when data is integrated into complex machine learning models.

To tackle these challenges, India must adopt a comprehensive, multi-layered framework that goes beyond traditional data protection. This should include the introduction of AI-specific laws that differentiate between various data processing technologies and require transparency, accountability, and redress mechanisms. There should also be a stronger focus on ethical AI design, ensuring fairness, inclusion, and human oversight in technological development. Additionally, efforts to enhance public discourse and digital literacy will help citizens understand how their data is used, challenge unethical practices, and regain control over their digital identities in an increasingly algorithm-driven world.

References

1. *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, (2017) 10 SCC 1, AIR 2017 SC 4161, available at https://indiankanoon.org/doc/127517806/.

2. Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India), available at https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf.

3. Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

4. UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 41 C/Res. 37 (Nov. 24, 2021), available at https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence.

5. OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (May 22, 2019), available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

6. Anirudh Burman, *Understanding India's New Data Protection Law*, Carnegie Endowment for Int'l Peace (Oct. 2023), available at https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law.

7. Right to Be Forgotten, Drishti IAS (Aug. 5, 2024), available at https://www.drishtiias.com/daily-updates/daily-news-analysis/right-to-be-forgotten-7.

8. *Studio Ghibli Has Few Legal Options to Stop OpenAI from Ripping Off Its Style*, Bus. Insider (Mar. 2025), available at https://www.businessinsider.com/studio-ghibli-openai-chatgpt-image-feature-copyright-law-2025-3.

9. OpenAI, *DALL·E: Creating Images from Text* (Jan. 5, 2021), available at https://openai.com/index/dall-e/.

10. IndiaAI, *Report on AI Governance Guidelines Development*, available at https://indiaai.gov.in/article/report-on-ai-governance-guidelines-development.

11. Amlan Mohanty & Shatakratu Sahu, *India's Advance on AI Regulation*, Carnegie Endowment for Int'l Peace (Nov. 21, 2024), available at https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation.

12. Truyo, *India's Draft AI Governance Act: A New Era of Regulation* (June 2024), available at https://truyo.com/indias-draft-ai-governance-act-a-new-era-of-regulation/.

13. Latham & Watkins LLP, *India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison* (Dec. 2023), available at https://www.lw.com/en/insights/2023/12/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.

14. Int'l Covenant on Civil & Political Rights art. 17, available at https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

15. Universal Declaration of Human Rights art. 12, available at https://www.un.org/en/about-us/universal-declaration-of-human-rights.