# **Rules and Regulations For AI**

## **USA**

* The Blueprint for an AI Bill of Rights is a set of five principles and associated practices to help guide the design, use, and deployment of automated systems to protect the rights of the American public in the age of artificial intelligence.

1. SAFE AND EFFECTIVE SYSTEMS

* Automated systems should be developed with consultation from diverse communities, stakeholders, and domain experts to identify concerns, risks, and potential impacts of the system.
* Systems should undergo pre-deployment testing, risk identification and mitigation, and ongoing monitoring that demonstrate they are safe and effective based on their intended use, mitigation of unsafe outcomes including those beyond the intended use, and adherence to domain-specific standards.
* Independent evaluation and reporting that confirms that the system is safe and effective, including reporting of steps taken to mitigate potential harms, should be performed and the results made public whenever possible.
* Systems should undergo extensive testing before deployment. This testing should follow domain-specific best practices, when available, for ensuring the technology will work in its real-world context.
* Testing conditions should mirror as closely as possible the conditions in which the system will be deployed, and new testing may be required for each deployment to account for material differences in conditions from one deployment to another.
* Avoid inappropriate, low-quality, or irrelevant data use and the compounded harm of its reuse. Data used as part of any automated system’s creation, evaluation, or deployment should be relevant, of high quality, and tailored to the task at hand.
* Derived data should be viewed as potentially high-risk inputs that may lead to feedback loops, compounded harm, or inaccurate results. Such sources should be carefully validated against the risk of collateral consequences.
* Data reuse, and especially data reuse in a new context, can result in the spreading and scaling of harms. Data from some domains, including criminal justice data and data indicating adverse outcomes in domains such as finance, employment, and housing, is especially sensitive, and in some cases its reuse is limited by law.
* Independent evaluators, such as researchers, journalists, ethics review boards, inspectors general, and third-party auditors, should be given access to the system and samples of associated data, in a manner consistent with privacy, security, law, or regulation (including, e.g., intellectual property law), in order to perform independent evaluations.

1. ALGORITHMIC DISCRIMINATION PROTECTIONS

* You should not face discrimination by algorithms and systems should be used and designed in an equitable way.