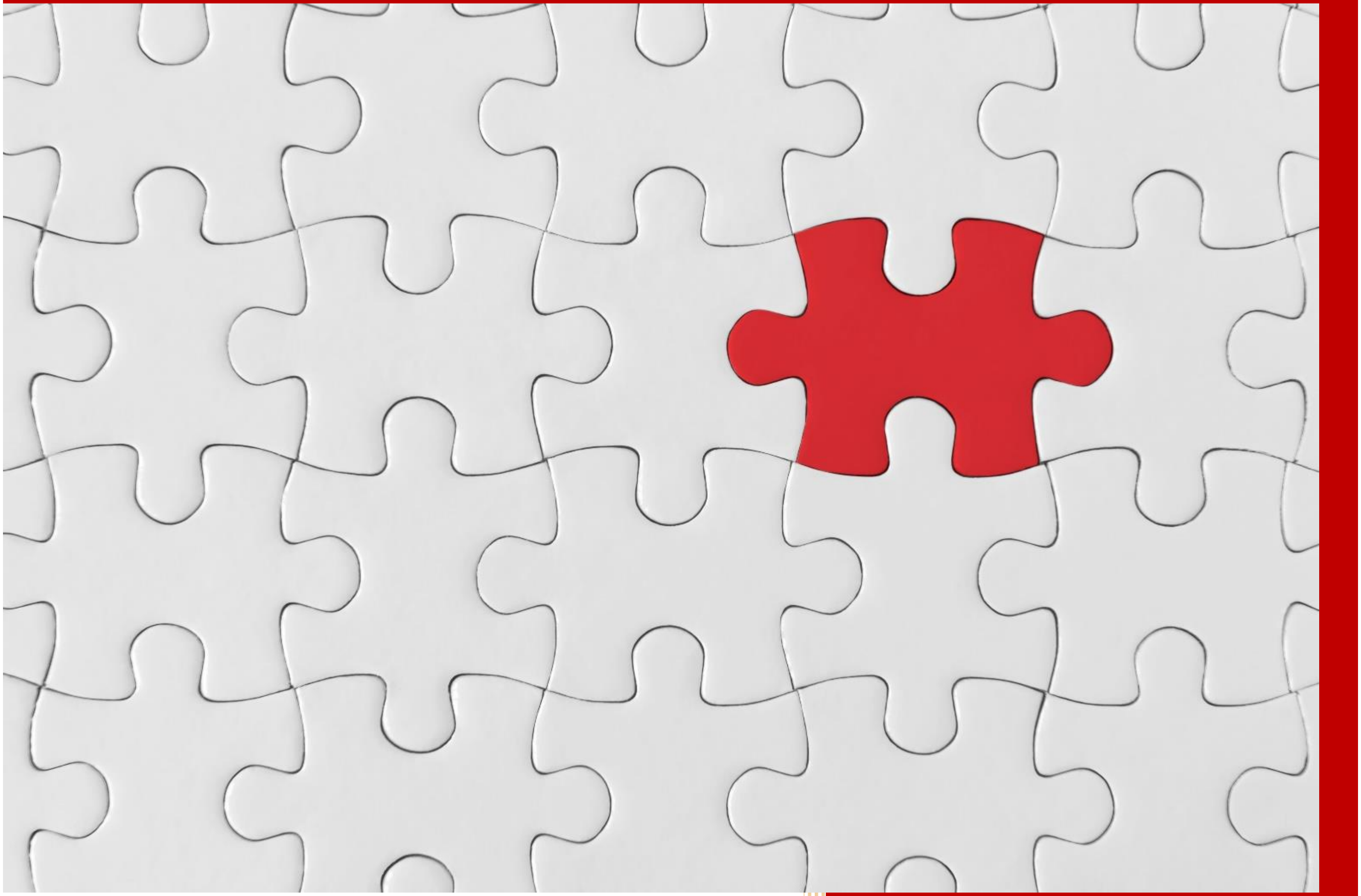
2023

Fundamental Rights Impact Assessment



Kosha Doshi

EU Digital Partners

10/10/2023

OVERVIEW - EUROPEAN ARTIFICIAL INTELLIGENCE (EU AI) ACT

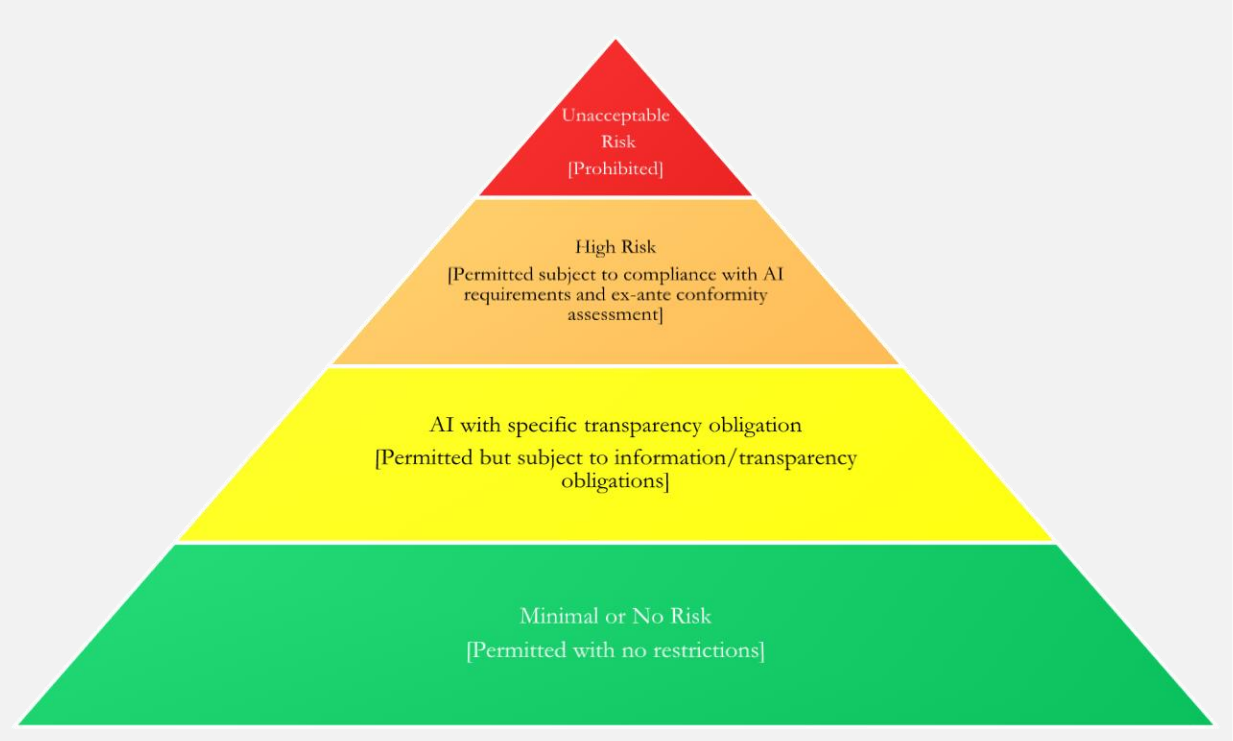
The AI Act represents a groundbreaking legal framework, marking a significant milestone in the regulation of artificial intelligence. It stands as the first comprehensive set of rules and obligations aimed at addressing the potential risks associated with AI, with a primary focus on safeguarding the well-being, safety, and fundamental rights of not only European Union (EU) citizens but also extending its impact beyond EU borders. Its global implications for AI governance cannot be overstated.

Leading up to the crucial vote on the AI Act in the European Parliament, various stakeholders from civil society came together to emphasize the importance of prioritizing fundamental rights and ensuring robust protection for individuals affected by AI systems. The proposed amendments seek to establish stringent obligations for users of high-risk AI, enhancing foresight, transparency, and accountability for those influenced by these advanced technologies. The key amendments in question include:

1. **Obligation to Define Affected Persons:** Users of high-risk AI will be required to clearly define the individuals or groups who may be impacted by the system's operation.
2. **Fundamental Rights Impact Assessment:** Users of high-risk AI will be obligated to conduct and publicly disclose a comprehensive assessment of the system's impact on fundamental rights. This assessment will encompass vital aspects such as the system's intended purpose, geographical and temporal scope, legality, compatibility with accessibility regulations, anticipated direct and indirect effects on fundamental rights, potential risks to marginalized individuals or those vulnerable to discrimination, environmental consequences, other adverse impacts on the public interest, and a detailed plan for mitigating identified harms along with an evaluation of the effectiveness of these mitigation measures.

TYPES OF RISKS IN EU AI ACT

The EU AI Act is anchored by its robust risk categorization system, which serves as the cornerstone of AI regulation. This system classifies AI systems based on the extent of risk they pose to the well-being, safety, and fundamental rights of individuals. It's a nuanced approach, consisting of four categories: "unacceptable," "high," "limited," and "minimal/none."


Unacceptable
Risk
[Prohibited]
High Risk
[Permitted subject to compliance with AI requirements and ex-ante conformity assessment]
AI with specific transparency obligation
[Permitted but subject to information/transparency obligations]
Minimal or No Risk
[Permitted with no restrictions]

Unacceptable Risk Systems - A Strict Prohibition

Within the "unacceptable" risk category, AI systems face an outright ban. This decisive step has been taken in alignment with consensus among the three proposals. Systems in this category are those with a significant potential for manipulation. This manipulation can manifest through subtle subconscious messaging, stimuli, or by exploiting vulnerabilities related to factors such as socioeconomic status, disability, or age. Notably, AI systems used for social scoring, a practice that evaluates and categorizes individuals based on their behavior, are strictly prohibited. Furthermore, the European Parliament intended to prohibit real-time remote biometric identification in public spaces, including live facial recognition systems, as well as other biometrics and law enforcement applications.

High Risks Systems - Rigorous Regulation

AI systems classified as "high risk" fall into two key categories. First, they include systems that serve as a safety component or fall under the purview of existing safety standards and assessments, such as toys or medical devices. Second, they encompass AI systems used for specific sensitive purposes. While the precise list of these use cases may evolve it is currently understood to encompass eight high-level areas, which span:

1. Biometrics,
2. Critical infrastructure,
3. Education and vocational training,
4. Employment and workforce management,
5. Access to essential services,
6. Law enforcement,
7. Migration, asylum, border control management, and
8. Administration of justice and democratic processes.

Developers of high-risk AI systems are required to meet stringent requirements to demonstrate that their technology poses no significant threat to health, safety, or fundamental rights. These requirements include comprehensive risk management, robust data governance, continuous monitoring, meticulous record-keeping, detailed documentation, transparency, human oversight obligations, and standards for accuracy, robustness, and cybersecurity. Additionally, high-risk AI systems must be registered in a publicly accessible EU-wide database.

Limited Risk - Transparent Compliance

AI systems posing limited risk to individuals, such as Chatbots, Generative AI, and Algorithmic System that create or manipulate images, audio, or video content (e.g., deepfakes), are subject to transparency requirements. These requirements mandate disclosure that the content has been generated by AI.

Minimal Risk - No Restrictions

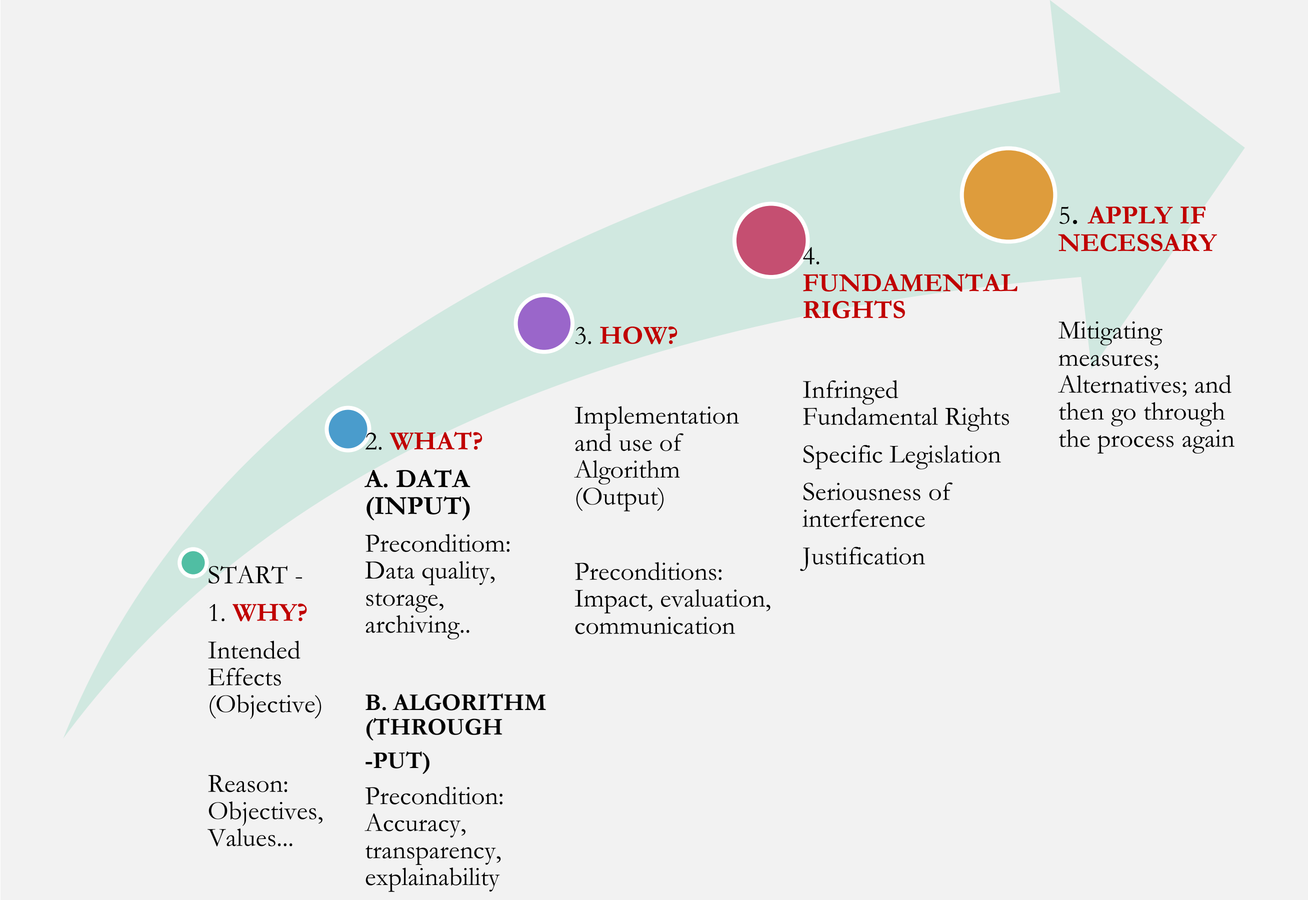
Finally, AI systems categorized as "minimal risk" or "low risk," including those used in computer games and AI-based spam filters, are not subject to any restrictions. These systems constitute the majority of AI systems currently in use in the market as of 2023.

INDIVIDUAL FUNDAMENTAL RIGHTS UNDER EU CHARTER

Every European Union (EU) citizen is granted a set of fundamental rights, all firmly rooted in values such as equality, non-discrimination, inclusion, human dignity, freedom, and democracy. These values are the bedrock of the EU, safeguarded by the rule of law, and enshrined in both the EU Treaties and the Charter of

Fundamental Rights. The EU Charter of Fundamental Rights is a proclamation jointly established by the European Parliament, the Council, and the Commission. It serves as a foundation upon which the EU is constructed, emphasizing essential principles like human dignity, freedom, equality, and solidarity. Within a single comprehensive document, the Charter outlines a wide spectrum of civil, political, economic, and social rights enjoyed by both Union citizens and all individuals residing within the EU's territory. When conducting Fundamental Rights Impact Assessments (FRIA), it is crucial for the Ethics Committee to thoroughly evaluate any possible direct or indirect effects on each of these Fundamental Rights.

FUNDAMENTAL RIGHTS IMPACT ASSESSMENT



START -

1. **WHY?**

Intended Effects (Objective)

Reason: Objectives, Values...

2. **WHAT?**

A. DATA (INPUT)

Preconditiom: Data quality, storage, archiving..

B. ALGORITHM (THROUGH-PUT)

Precondition: Accuracy, transparency, explainability

3. **HOW?**

Implementation and use of Algorithm (Output)

Preconditions: Impact, evaluation, communication

4. **FUNDAMENTAL RIGHTS**

Infringed Fundamental Rights

Specific Legislation

Seriousness of interference

Justification

5. **APPLY IF NECESSARY**

Mitigating measures; Alternatives; and then go through the process again

WHAT (DESCRIBING SCOPE)

The Ethics Committee's role encompasses several crucial aspects of the Algorithmic system's implementation. Firstly, it should clearly define the geographic scope within which the Algorithmic system will be utilized. This involves setting precise boundaries that delineate what falls within the purview of the Fundamental Rights

Impact Assessments (FRIA) and what does not. These boundaries extend to any associated ecosystem that either provides support to, receives support from, or integrates with the Algorithmic system.

Additionally, the ethics committee must carefully consider the nature of the data that the Algorithmic system will handle, including any special category or criminal offense data. Evaluating the quantity of data collected and employed by the system is pivotal, as is understanding the rationale behind the necessity of this personal data. Furthermore, the committee must establish the duration for which personal data will be retained and specify the corresponding data retention periods. Furthermore, the ethics committee should conduct a comprehensive examination to determine the potential impact on individuals resulting from the Algorithmic system's operation. This entails assessing both the likely and potential number of individuals who may be affected and also taking into account the frequency of processing operations.

HOW (DESCRIBING NATURE)

The Ethics Committee's responsibility encompasses providing a comprehensive description of the algorithmic system. This description should encompass the inherent nature of the algorithmic system and explicitly identify any deliberate or inadvertent inputs and feeds that have the potential to influence or alter the expected results or outputs generated by the algorithmic system. Such alterations could potentially impact an individual's Fundamental Rights. For example, this may involve variable effects on an Automated Employment Decision Tool (AEDT) when processing CVs submitted in different languages or fonts. Furthermore, the Ethics Committee is tasked with ensuring that the algorithmic system remains accessible to users and that it offers adequate explainability. This is crucial in order to provide users and affected individuals with a clear understanding of how the system operates.

Additionally, the Ethics Committee must delineate the procedures governing data handling by the algorithmic system. This encompasses how data is collected, utilized, stored, and eventually deleted. It is imperative to specify the sources of data and assess whether the data sources carry a high risk to individuals. The committee should also deliberate on who will be granted access to this data and whether any data sharing arrangements with external parties or alternative uses, such as retraining the algorithmic system or data monetization, are anticipated. To enhance comprehension, the Ethics Committee may opt to incorporate visual aids such as diagrams or alternative methods to illustrate the data flows within the algorithmic system. This will aid in providing a more lucid depiction of the system's functioning.

WHO (DESCRIBE CONTEXT)

The Ethics Committee is tasked with providing a comprehensive overview of the Algorithmic System. This entails elucidating the system's contextual background and clarifying whether it has been tailored for a specific industry or sector, such as healthcare, finance, or government. Furthermore, the committee should identify the key stakeholders who will interact with or be affected by the Algorithmic System. In particular, they should pay special attention to vulnerable groups that may require special adjustments or additional protective measures. An essential aspect that the Ethics Committee must deliberate upon is the nature of the relationship between the individuals utilizing or being impacted by the Algorithmic System. This includes employees, customers, and other relevant parties. It is crucial to ascertain whether these individuals anticipate their data being employed in the manner prescribed by the system. Additionally, the level of control that individuals will retain over the Algorithmic System warrants careful consideration.

The Committee must also evaluate the present state of technology and its maturity within the relevant field. This assessment should encompass a review of any potential concerns, be they of a public, ethical, or security nature, associated with the deployment of this type of Algorithmic System. These concerns should be factored into the decision-making process to ensure the responsible and ethical use of the system by individuals and organizations alike.

WHY (DESCRIBE PURPOSE)

The ethics committee's role is to provide a comprehensive description of the intended purpose behind the utilization of the Algorithmic system, as well as to establish a clear objective for the system. Within this framework, the committee must take into account the organization's overarching business goals and what it aims to accomplish through the implementation of this system. Moreover, the committee should delineate the anticipated effects on individuals, including any potential advantages for those who use the system, as well as the impacts on individuals, the organization itself, and society at large. In order to maintain a sense of purpose and scope, the committee is responsible for ensuring that the utilization of the Algorithmic system is essential to achieving the stated objectives. Additionally, they must confirm that there are no alternative methods that are less invasive or impactful that could be employed to attain the same goal.

HOW LONG (LIFE EXPECTANCY)

The ethics committee must provide a comprehensive delineation of the expected timeframe for the utilization of the Algorithmic system and its anticipated duration in the market without substantial alterations. In this context, it is essential for the ethics committee to deliberate on the criteria for identifying when a noteworthy transformation in the system's design or purpose has transpired. Additionally, the committee should take into account potential alterations in technology, legal regulations, market conditions, business goals, and other pertinent factors that could necessitate a substantial modification sooner than initially foreseen or potentially impact the anticipated lifespan of the system.

CATEGORIES OF AFFECTED INDIVIDUALS

The ethics committee's role involves discerning the various categories of individuals and groups, such as employees, customers, members, students, etc. who might potentially experience the effects of the Algorithmic system. Furthermore, the committee should delineate the categories of individuals and groups who will utilize the Algorithmic System, if distinct from those being affected by it. Additionally, they should examine any potential biases or relationships between these groups and individuals, such as teachers implementing an Algorithmic System that could affect their students or police officers employing an Algorithmic System that might impact suspects.

VERIFICATION OF RELEVANT LEGAL FRAMEWORKS

The Ethics Committee plays a crucial role in ensuring that the Algorithmic System aligns with both European Union and national legislation pertaining to fundamental rights. In doing so, the committee takes special care to consider the potential differential impact of the Algorithmic System on vulnerable groups compared to the broader population. This meticulous examination serves to uphold the principles of non-discrimination, as mandated by European and national anti-discrimination laws. It is paramount to emphasize that vulnerable groups often enjoy specific rights safeguarded by the EU Charter of Fundamental Rights, as well as by national and international statutes such as the United Nations Convention on the Rights of the Child. These rights necessitate a profound understanding of individual vulnerabilities and the provision of necessary protection and care to ensure their well-being.

Furthermore, the Ethics Committee should not overlook the fundamental right to a high level of environmental protection enshrined in the EU Charter of Fundamental Rights. This aspect, too, must be taken into account during the evaluation process. In assessing the potential harm posed by the Algorithmic System, the Ethics Committee should also consider European Union and national policies, particularly with regard to the health and safety of individuals. This comprehensive approach ensures that the ethical and legal dimensions of the Algorithmic System are rigorously evaluated and upheld, promoting fairness, inclusivity, and the protection of individual rights.

IDENTIFYING FORESEEABLE IMPACT AND DEFINING SERIOUSNESS

When deploying the Algorithmic System into operation, the ethics committee's foremost responsibility is to meticulously assess its potential impact on fundamental rights and the specific risks it may pose to vulnerable groups. In this endeavor, they must ascertain whether these impacts are uniform across different categories of individuals and groups or if disparities exist, elucidating the underlying reasons for any variations. Notably, this process is obligatory for large organizations and discretionary for SMEs, with the former mandated to notify the national supervisory authority, relevant stakeholders, and representatives of affected individuals or vulnerable groups (e.g., equality bodies). These stakeholders are granted a six-week window to provide their insights, which are duly documented as part of the impact assessment.

The ethics committee should be diligent in exploring the interplay between Algorithmic System users and those who may be affected by the system's outputs. It is imperative to unearth potential conflicts and discern any risks or issues that could skew inputs or outputs, thereby altering the impact of Algorithmic System on individuals. For instance, these biases could manifest as teachers favoring their pupils in the case of educational Algorithmic System or police officers unfairly influencing outcomes concerning suspects.

The ethical evaluation process is outlined in four steps:

- **Step 1:** Identify the fundamental rights applicable to individuals directly or indirectly impacted by the Algorithmic System.
- **Step 2:** Identify vulnerable groups whose fundamental rights may be differentially affected.
- **Step 3:** Delve into the actual or potential impact on individuals' fundamental rights, scrutinizing variances between vulnerable groups and any bias-driven disparities arising from the user-group relationships.
- Step 4a: Gauge the severity of interference with fundamental rights for each identified vulnerable group, categorizing risks by their severity (e.g., Serious, High, Medium, Low, None).
- Step 4b: Determine the likelihood of each identified risk to fundamental rights for each vulnerable group, grading them based on the likelihood of occurrence (e.g., Persistent, Likely, Possible, Unlikely, Rare).
- **Step 4c:** Combine the severity and likelihood scores to ascertain the overall risk to individuals, denoting the seriousness of the risk (e.g., High Risk, Medium Risk, Low Risk).

Furthermore, the ethics committee must give meticulous consideration to the reasonably foreseeable adverse impact that the Algorithmic System may have on the environment, as stipulated in Article 37 of Fundamental Rights. A paramount objective is to ensure that the Algorithmic System actively promotes a high level of environmental protection and contributes to enhancing environmental quality. To achieve this, environmental considerations should be integrated into organizational policies, encompassing areas such as climate change, biodiversity preservation, water conservation, air and noise pollution control, waste management, integrated pollution prevention, and control, integrated product policies, and environmental liability. This includes scrutinizing the processing power and energy consumption employed by data centers for training and operating the Algorithmic System.

Similar to the assessment of fundamental rights, the engagement process for environmental impact involves distinct steps:

- **Step 1:** Identify any environmental impact directly or indirectly attributable to the Algorithmic System.
- **Step 2:** Specify the actual or potential impact on the environment.
- **Step 3a**: Evaluate the severity of the impact on the environment, ranking risks by their severity (e.g., Serious, High, Medium, Low, None).
- **Step 3b:** Determine the likelihood of each identified environmental risk, grading them based on the likelihood of occurrence (e.g., Persistent, Likely, Possible, Unlikely, Rare).
- **Step 3c:** Aggregate the severity and likelihood scores to ascertain the overall risk to the environment, with classifications ranging from High Risk to Low Risk.

In cases where the Algorithmic System affects or has the potential to threaten the environment, it is incumbent upon organizations to implement additional requirements and mitigations aimed at minimizing these risks.

MITIGATING IDENTIFIED RISKS

The Ethics Committee is tasked with crafting a comprehensive strategy to address and alleviate any potential or actual harm and adverse impacts on an individual's fundamental rights within the organization's operations. This strategy encompasses the identification of specific measures and mitigations that the organization can adopt to counter the risks identified. It is crucial to recognize that these mitigation efforts may vary across different groups of individuals, particularly those who are marginalized or belong to vulnerable communities. The following steps outline this mitigation process:

- **Step 1:** Establish the criteria for determining an acceptable level of risk.
- **Step 2:** In cases where risks surpass the acceptable threshold, the Ethics Committee shall identify potential measures and mitigations that could be put in place to reduce these risks for individuals affected by the Algorithmic System. The goal is typically to either eliminate, reduce, transfer, or accept the risk.

- **Step 3:** Determine the residual risk that will persist after the implementation of proposed measures and mitigations. This residual risk should strike a reasonable balance between the organization's objectives and the potential infringement on fundamental rights.
- **Step 4a:** Assess the severity of any remaining risks to fundamental rights for each vulnerable group identified. These risks should be graded based on their impact severity (e.g., Serious, High, Medium, Low, None).
- **Step 4b:** Evaluate the likelihood of any remaining risks to fundamental rights for each identified vulnerable group, categorizing them according to the likelihood of occurrence (e.g., Persistent, Likely, Possible, Unlikely, Rare).
- **Step 4c:** Combine the severity and likelihood scores to determine the overall residual risk to individuals. This overall risk assessment should be graded in terms of seriousness (e.g., High, Medium, Low Risk).
- **Step 5:** Make a judgment regarding the implementation of proposed measures and mitigations, considering factors such as cost, time, and effort needed versus the potential reduction of risk. Document the rationale for either implementing or not implementing these measures.
- **Step 6**: Put any agreed-upon measures and mitigations into practice. Once all these mitigations have been applied, the Ethics Committee must ascertain whether the risks to individuals have been adequately reduced to enable the Algorithmic System to be put into operational use.

If it becomes evident that the risks to individuals cannot be effectively mitigated, or if there are concerns that using the Algorithmic System in accordance with the provider's instructions may pose a risk as defined in Article 65(1), the organization must take immediate action. Specifically, they should promptly inform the provider or distributor and notify relevant national supervisory authorities. Furthermore, they should refrain from deploying the high-risk Algorithmic System until the situation is resolved satisfactorily.

MONITORING CONTROLS, RISK TREATMENTS AND MITIGATIONS

The Ethics Committee holds the responsibility of crafting comprehensive documentation that outlines the organizational governance framework. This documentation serves as a blueprint delineating the operational aspects of governance, oversight, and accountability systems. It also provides insight into the composition of the expert team, specially trained to comprehend the multifaceted risks associated with Algorithmic Systems, including but not limited to risks concerning individual rights and freedoms, privacy by design, and data protection.

Within this framework, the committee must ensure the establishment of a robust monitoring system. This system is essential for continuously supervising the effectiveness of controls, risk treatments, and mitigations aimed at reducing risks to individuals. Moreover, effective procedures must be in place to assess the performance of these controls, risk treatments, and mitigations. This step is particularly critical because the Algorithmic System, subject to a Fundamental Rights Impact Assessment (FRIA), inherently carries a 'high-risk' designation until mitigations are fully integrated. Therefore, it is imperative to monitor the efficacy of these measures.

The committee's responsibilities also extend to evaluating and documenting the mechanisms for human oversight. This entails defining the circumstances under which human oversight comes into play, such as timely spot checks or alerts triggered when certain thresholds are exceeded. Additionally, the documentation should elucidate the nature and role of human oversight, and if issues are identified by human operators, it should outline the steps taken to remediate such issues to prevent their recurrence.

In recognition of the importance of addressing concerns from various stakeholders, the committee must ensure the existence of a well-defined process for receiving, handling, logging, and monitoring complaints. The organizational complaints procedure should encompass details on how individuals can submit complaints, the designated authorities or channels for complaint resolution, and the escalation process for unresolved issues.

Furthermore, it is incumbent upon the Ethics Committee to demonstrate a keen awareness of considerations when dealing with complaints from vulnerable groups. This involves assessing issues related to accessibility and sensitivity to the potential impact on the individual. Different categories of individuals and groups may experience varying levels of impact, and what might appear as a minor complaint for one individual could constitute an emergency situation for another, particularly within vulnerable groups.

The complaints procedure should also delineate the systematic steps taken to achieve resolution, including the specific criteria governing redress for individuals, with due consideration for potential disparities in redress mechanisms for vulnerable groups. This holistic approach ensures that the governance framework not only addresses operational aspects but also embraces a comprehensive understanding of risks, accountability, and inclusivity.

ESTABLISH THRESHOLDS OF MONITORING

The Ethics Committee bears the crucial responsibility of not only instituting robust metrics, measurements, and thresholds but also continually monitoring their efficacy in reducing the risks posed by the Algorithmic System and its potential impact on the fundamental rights of individuals. Furthermore, the committee must establish the criteria that trigger human oversight of the AS, defining the thresholds that necessitate human intervention.

In parallel, the committee should implement metrics, measurements, and thresholds to oversee the resolution of complaints effectively. It's essential to gauge the efficiency of the complaint resolution process. One of the committee's key tasks is to evaluate whether safety thresholds should be tailored to diverse individual categories, including vulnerable groups. Recognizing that different categories and groups may experience varying degrees of impact, what might be considered safe for one category could pose risks to a member of a vulnerable group.

In the event that the defined thresholds are exceeded to a degree where the organization has legitimate reasons to believe that using the Algorithmic System in accordance with the provider's instructions may result in the Algorithmic System presenting a risk as defined in Article 65(1), a well-defined procedure must be activated. This involves notifying the provider initially, followed by the importer or distributor, and relevant national supervisory authorities. This process is imperative, especially when identifying any serious incidents or malfunctions as defined in Article 62, warranting an immediate halt to Algorithmic System usage. Additionally, organizations may consider documenting such incidents in the AI Incidents Database as a means of notifying individuals about potential risks associated with the Algorithmic System. This approach ensures transparency and facilitates information dissemination to relevant stakeholders, fostering a safer and more accountable AI ecosystem.

ESTABLISH FREQUENCY FOR REASSESSMENT

The obligation to conduct a Fundamental Rights Impact Assessment (FRIA) is applicable when initially deploying the high-risk Algorithmic System. However, it is imperative for organizations to maintain vigilant oversight of potential risks that could impact individuals' fundamental rights continually. To facilitate this ongoing vigilance, the Ethics Committee is tasked with establishing a reassessment frequency for the risks and mitigations identified in the Fundamental Rights Impact Assessments (FRIA). The reassessment frequency is not one-size-fits-all; rather, it varies depending on several factors, including the nature of the Algorithmic System and the potential harms and impacts on individuals. When the FRIA reveals substantial risks to individuals' fundamental rights, more frequent reassessments are warranted, with the frequency determined by the severity of the identified risks.

In cases that resemble previously assessed scenarios, organizations have the option to refer back to earlier conducted Fundamental Rights Impact Assessments (FRIA) or leverage existing assessments conducted by service providers. This approach streamlines the assessment process and ensures that valuable insights are not duplicated unnecessarily. Furthermore, certain organizations, as specified in Article 51 (e.g., public authorities or union institutions), are obligated to make the results of the Fundamental Rights Impact Assessments (FRIA) available to the public. This involves publishing a summary of the assessment outcomes as part of the registration of use, in accordance with their obligations under Article 51(2). This transparency is a crucial step in fostering accountability and ensuring that the public is informed about the impact of high-risk Algorithmic System on fundamental rights.

EU Digital Partners, Regulatory Compliance Services
Contact
+40 747489033
https://eudigitalpartners.com/
pp@eudigitalpartners.com

Author
Kosha Doshi
Final Year Law Student Symbiosis Law School, Pune, India & Legal Intern
Data Privacy and Digital Law at EU Digital Partners
https://eudigitalpartners.com/