International Journal of Advance and Applied Research

www.ijaar.co.in

ISSN – 2347-7075 Impact Factor – 7.328

Peer Reviewed Bi-Monthly

Vol.10 No.3 January – February 2023

IMPLEMENTATION OF GOVERNANCE MODELS WITHIN ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Derrick Francis[1] &Dr. Pankaj Jain[2]

[1]*Ph.D. Research Scholar, Department of Management, Shri. J.J.T. University, Rajasthan, India*

[2]*Professor & Ph.D. Research Guide, Department of Management,Shri J.J.T. University,Rajasthan,India*

Corresponding Author -Derrick Francis

DOI - 10.5281/zenodo.7894655

Abstract:

An organization largely reliant on artificial intelligence (AI) is not adequately protected against cyberattacks. Organizations are responsible for ensuring their goods and services are available, reliable, quality, and safe regardless of the usage of AI technology. Implementation of governance models within artificial intelligence (AI) technologies is essential for ensuring that AI systems are developed and used in an ethical and responsible manner. A governance framework should be established to define the roles and responsibilities of all stakeholders involved in the development, deployment, and use of AI systems. This framework should also establish guidelines for ensuring the ethical and responsible use of AI, including addressing issues such as bias, transparency, accountability, and privacy. The development of ethical and responsible guidelines for AI is critical for ensuring that AI systems are developed and deployed in a way that benefits society as a whole. Such guidelines should be designed to protect the rights and interests of stakeholders, including individuals, organizations, and communities. Additionally, governance models must be adaptable to evolving AI technologies, as well as changing social and ethical norms. As AI technologies continue to evolve and become more complex, the need for effective governance models will only become more important, and stakeholders must work together to develop and implement these models to ensure that AI systems are developed and used in a responsible and beneficial way.

Keywords: Governance models, Artificial intelligence, Technologies, Organizations.

Introduction:

In this part, the concept of governance and the underlying ideas are explained. To begin with, this part examines the official and informal standards of conduct that regulate behaviour in public spaces, and the ways in which these standards are influenced by ethical concerns, market circumstances, and social customs. Second, the attention shifts to a particular set of formal principles, namely the norms of legal regulation, which we differentiate between top-down regulation, co-regulation, and self-regulation. This section focuses on the ethical and moral principles of AI4People's 2018 Ethical Framework and how legal legislation and governance interact with them.

Managerial Model:

Structures of Internal Governance:

As a consequence, enterprises should design an internal governance structure for artificial intelligence research and use. An AI strategy and an AI governance committee should be part of the internal governance framework (or a similar body). Companies should adopt rules for the application of privacy and data security by design throughout the AI life cycle since AI systems need vast amounts of data, some of which may be personal. Existing frameworks for data governance or accountability, such as the PCPD's Privacy Management Program, might be used and adapted, and components of this Guidance could be included into the current workflow to easily oversee the creation and usage of AI systems. Structure of the Government Inherent concepts: Human oversight / Accountability.

The Complexity of AI governance:

There are many ethical concerns to consider when designing an AI governance system, and it is difficult to determine which regulatory instrument is most appropriate. Additionally, there are complex interactions between relevant technology, the market, individuals, society and the environment that must be considered, and ultimately politics and regulation must be taken into consideration. To put it another way, creating an artificial intelligence governance system is incredibly tough.

Artificial Intelligence (AI) research and application need expertise in a wide range of topics from computer engineering to data science and cybersecurity. The execution of the AI plan should be overseen by an internal governance structure that has adequate resources, experience, and authority. The following are possible components of an AI governance structure:

The principles:

Canada's approach to AI governance should accomplish the following to manage the conflict between fostering innovation and managing risks:

- A policy of responsible AI development and application that emphasises justice, equality, safety, security, economic and political stability as well as human wellbeing should be followed.
- Individual AI applications should be the focus of risk management and regulatory actions rather than AI as a whole.

- A declaration on the responsible development and use of AI should be written and endorsed to urge private sector developers and adopters, as well as public sector decision makers and civil servants, to put a high focus on justice, safety, security, and health. Consider using the Montreal Declaration's position on responsible AI development as a model for your own position on the new declaration.

Finding out how much of a role humans have in AI-augmented decision making:

AI risk appetite, i.e., what risks are tolerable and how much human involvement is appropriate in AI-augmented decision-making, may be determined using the method given here.

If an AI-based system makes judgments that have a major impact on a person's financial, legal, or other substantial interests, consider incorporating a right to an explanation. When considering whether or not to create a right, the EU's legal framework is a useful starting point (GDPR). A public discussion is necessary whether such a right should exist and if answers can be provided in a way that is technically viable. Individuals' rights and interests should be protected at the very least, and AI users in both the commercial and governmental sectors should be made aware of this. Theodore D. Munro (2019, January). Navigating risks, incentives, and uncertainties in AI governance. Similar governance mechanisms related to NeurIPS' larger effect criterion are discussed at the Public Policy Forum.

For insurance companies, this implies that they must also be open and honest about how they utilise their customers' personal information.

Interaction and communication with stakeholders Communication and relationship management strategies for an organization's stakeholders.

The third factor that makes AI-governance a challenging and time-consuming undertaking is the fact that all key factors are interconnected, either directly or indirectly. In the future, existing occupations may be replaced by new ones, there will be less social contact between humans and machines, and more raw resources will be used to build more machines.If you'd like to learn more about some of the issues that arise from the increased usage of AI and autonomous systems. However, new technologies also bring with them the potential for new economic possibilities, which in turn have the ability to create new markets or alter already existing ones. In certain cases, additional regulatory measures may be necessary due to the nature of the new technologies' consequences. A value judgement must be made in light of multiple, often even contradictory, basic concepts when it comes to regulation, on the other hand. Competition as a presumed driver of consumer and public welfare, as well as other fundamental normative concepts represented in basic rights, constitutional principles, and ethics are included.

As a result of these stakeholders' interconnectedness, there is a great deal of difficulty in dealing with any of their actions or reactions. Regulators may also have an influence on the dynamics of innovation. However, regulation may encourage the development of new technologies and business models based on technology. As previously said, data privacy legislation is an example of a policy that limits the free use of personal data while also encouraging firms to build privacy-by-design solutions and therefore contributing to a high degree of data protection.

Consumer decision-making can be aided by AI systems, and insurance companies are well-positioned to create and explain these advantages while still upholding the ideal of human autonomy. Artificial intelligence (AI) may have both positive and negative consequences, and this must be taken into consideration when implementing techniques that aim to maximise customers' "willingness to pay" and "willingness to accept," such as using AI in pricing and claim optimization. For vulnerable customers and protected groups, negative impacts are of particular concern.

Inequity, Partiality, and Racial Profiling:

The relevance of the problem Unfairness Smith, L (2017).(Unfairness by algorithm: Distilling the harms of automated decision-making.Future of Privacy Forum.https://fpf.org/2017/12/11/ unfairness- by- algorithm- distilling- the- harms- of- automated- decision- making.),bias (Courtland 2018). Bias detectives are academics who are working to make algorithms more equitable. A number of issues have been raised about algorithms and automated decision-making systems, such as those used to make health-care decisions, such as questions about the impact of nature and bias. (Smith 2017) Statistical bias may be introduced into algorithms for self-driving vehicles. Article 21 of the EU Charter of Fundamental Rights enshrines the concept of nondiscrimination, which must be taken into consideration when algorithms are applied in daily life (FRA 2018). According to the most current version of the FRA (FRA 2018), instances of possible discrimination include automated selection for employment interviews, risk assessments in creditworthiness or trials, and a variety of other situations. The European Parliament has commissioned a study on data mining in order to better understand the consequences of data mining for basic rights. "Because of the data sets and algorithmic systems used when making assessments and predictions at the various stages in the process of data processing," according to a statement from the European Parliament (2017), big data may result in "not only infringements of fundamental rights of individuals, but also differential treatment of and in-direct discrimination against groups of people who share similar characteristics."

In order to build trust among all parties involved in the insurance process, it is critical to make use of data. There should be no information gathered or maintained unless it is absolutely essential to achieve the identified objectives, and that information should be relevant to those purposes. Insurance companies now have access to new and more sensitive personal data, as well as data from the Internet of Things' vehicle telematics, wearable medical devices, and social media (IoT). This information must be used in a fair way to preserve people's privacy.

Proposed solutions/the manner in which it is being handled:

There was a call to action from the EC, Member States, and data protection authorities in the research. “to identify and take any possible measures to minimise algorithmic discrimination and bias and to develop a strong and common ethical framework for the transparent processing of personal data and automated decision-making that may guide data usage and the ongoing enforcement of Union law” EP (2017).

Various suggestions have been put up to deal with these concerns. If, for example, you do regular assessments of data sets' representativeness and their potential for bias, you'll be taking the right steps. On the way to discrimination-aware data mining, it is important to keep humans in the loop and under the microscope (Big data, 5 (2), 135–152), in addition to making algorithms accessible to the general audience. Techniques for confirming that algorithmic decision systems do not display unjustifiable biases in a systematic way are being developed. The IEEE P7003 Standard for Algorithmic Bias Considerations, which is being created as part of the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, may assist anybody working on algorithmic systems, whether independently or as part of an organization. It is intended to provide individuals or organizations building algorithmic systems with a development framework in order to avoid unwanted, unjustified, and unnecessarily discriminating effects for its users. There are also a variety of open source toolkits available, such as the AI Fairness 360 Open Source Toolkit, which helps users discover, report, and mitigate discrimination and bias in machine learning models across the life cycle of an AI application. Other open source toolkits, such as the AI Fairness 360 Open Source Toolkit, are also available. This method employs over 70 fairness criteria as well as ten of the most advanced bias reduction algorithms created by academics.

Intellectual property rights are a concern:

The nature of the issue and its importance are explained. International treaties, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social, and Cultural Rights, and the (VDPA). As the World Intellectual Property Organization (WIPO) puts it, these rights have been "contextualized in a range of policy domains" (1998). Intellectual property issues arise as a result of AI, such as who owns the works or ideas created or generated by AI. Is artificial intelligence a kind of art in and of itself? Which party controls the data gathering from which artificial intelligence must learn, and how? In cases when AI-created creativity or innovation infringes on the rights of others or violates other legal restrictions, who has the burden of proving that the AI is responsible?

Solutions that have been proposed/the manner in which it is being handled:

The law may be able to give a number of different remedies to the problems mentioned. R. Rodrigues, Ph.D. (2019): A study of the legal and human rights needs for robotics and artificial intelligence is being carried out as part of the SIENNA project as part of its legal and human rights component. In the United Kingdom, computer-generated literary, musical, and theatrical works are protected under the Intellectual Property (Protection) Act. A person who creates an artificial intelligence design retains ownership of such rights unless the work was commissioned or produced as part of an employment agreement. This second situation, as described by the United Kingdom Copyright Service (2004), involves the ownership of intellectual property by the employer or organization that commissioned the AI work. Given that a registered trademark is a kind of personal property, an artificial intelligence system may be unable to exercise this right unless it is also capable of owning or possessing such property.

Employees are suffering from negative consequences:

The IBAGEI is a non-profit organization that promotes global employment (2017) Robotics and artificial intelligence in the workplace: what is the impact on employees? AI and robots are having a significant influence on the workplace, according to a new report Another important consideration is the possibility of employees losing their autonomy. Frontier Economics was published in 2018. On the Cusp of a Revolution in Economics (2018) The Royal Society and the Royal Academy of Engineering commissioned an assessment of the evidence on the impact of artificial intelligence on the workplace, which was carried out for them. In addition to having significant economic (for example, poverty) and social repercussions (for example, homelessness, displacement, violence, and despair), these problems have the potential to have a significant impact on human rights. They present ethical questions and difficulties that, although they may be difficult to answer, are still necessary to confront.

In order to fix this problem, a variety of options are being considered or have already been discussed. The UK House of Lords 2018 and the House of Lords Select Committee on Artificial Intelligence, for example in addition to a major revamp of the educational system The European Commission has published a report on artificial intelligence for Europe, which may be seen or downloaded from their website (2018) The European Union may be referred to in a variety of ways (2018a). the coordinated implementation of a plan that incorporates artificial intelligence The European Commission recommends that governments prioritize modernizing education at all levels, and that every European be given every opportunity to acquire the skills needed to prosper in their employment. For those who have lost their jobs due to the AI revolution, the Communication recommends that they get aid; the Communication says that "national efforts will be crucial for providing such up-skilling and training." Artificial Intelligence in Europe for the Year of 2018.In addition, it will be important to look into and restructure the social security systems.

Responsibilities In The Event Of Damage:

Describe the problem's nature and significance. People and property might be harmed by the deployment and usage of artificial intelligence technology. Who Is

Responsible When Artificial Intelligence Doesn't Work Out as Expected? a drone crashing with and destroying property, a medical software programme wrongly diagnosing and treating patients are only few instances of possible harms caused by autonomous vehicles). Because there are so many parties involved in an AI system (data providers, designers, manufacturers, programmers, developers, users and the AI itself), proving culpability when anything goes wrong is challenging and there are so many aspects to take into account, as they go on to say.

Solutions that have been proposed/the manner in which it is being handled:

Artificial intelligence liability problems might be handled within the ambit of either civil or criminal responsibility. Lawsuits using artificial intelligence are on the rise. This article looks at the possibility of criminal liability being imposed and who may be held liable in such an event. In addition, the question of whether artificial intelligence software is a product subject to design rules (for example, in the case of design or manufacturing faults) or a service subject to the negligence tort is examined in detail. If an artificial intelligence entity were to do harm, it might possibly be held legally liable. It asserts that criminal liability for intellectual property crimes perpetrated by artificial intelligence (AI) beings is a possibility, and it offers suggestions on how AI creatures should be prosecuted. Consumer protection legislation may also be able to resolve concerns of responsibility. Rachum-Twaig (2020). Whose robot is it anyway? SSRN proposes “supplementary rules that, together with existing liability models, could provide better legal structures that fit AI- based robots. Such supplementary rules will function as quasi-safe harbors or predetermined levels of care. Meeting them would shift the burden back to current tort doctrines. Failing to meet such rules would lead to liability. Such safe harbors may include a monitoring duty, built-in emergency breaks, and ongoing support and patching duties.” Rachum-Twaig argues that “these supplementary rules could be used as a basis for presumed negligence that complements the existing liability models”.

Operational Model:

Management of operations When designing, choosing, and maintaining AI models, including data management, there are a number of considerations.

Consumers' private habits and behaviors may be revealed in some datasets that are particularly sensitive. New datasets such as those gathered by wearables or automotive telematics devices, for example, might potentially be utilized for this purpose. Principles of Good Governance for AI in the EIS.

Those in the academic and non-profit sectors (Privacy International and Article 19 2018; Access Now 2018) This year's Access Now issue focuses on human rights. In certain cases, the scope of legal concerns relating to AI is extensive and includes a wide range of dangers and difficulties. Some of these are more general in scope, while others are more focused. Some analyses are based on a single domain. According to Price (Price 2017).

Algorithmic concealment:

How important the problem is, and why in legal debates around artificial intelligence, The absence of algorithmic transparency is a significant problem. Cath (2018) asserts that the rise of AI in high-risk areas like as healthcare and financial markets is driving an increasing demand for AI to be responsible, fair, and transparent. "Why that happened other than that a choice was taken by some software," which they suspected was the case, is what Desai and Kroll point out in their paper (2017). This is an issue. Information about the algorithms' operation is sometimes deliberately hidden from the public, which only serves to worsen the situation.

Data governance must be sound and transparent to guarantee that customers are treated fairly and non-discriminatory. Throughout the AI system's lifespan, insurance companies must check the accuracy, completeness, and appropriateness of the data they utilise. This is explained in depth in Chapter IX of this study. Personal information about clients must also be adequately communicated to them, and their approval must be sought before any use of such information is permitted" (noting that Article 6 GDPR also foresees other legal grounds for the processing of personal data). The techniques of data governance are described in depth in Chapters X and VIII, and they involve human control to ensure that the data is resilient and that it performs as intended. This chapter is concerned with the fair and nondiscriminatory use of data and artificial intelligence technologies. If a health insurer has the proper legal grounds to do so (such as customer consent), it can use customer data to provide customers with useful services, such as suggestions for improving driving skills or leading a healthy lifestyle. Patient data may also be required to research diseases and new healing concepts, as well as to provide insurance customers with tips for medical treatments. When you purchase a vacation package, you may be offered travel insurance products based on your bank account information or public social media postings. According to a study conducted by the EIOPA's Consultative Expert Group on Digital Ethics in Insurance-2021, artificial intelligence and its ethical and trustworthiness in the European insurance market are being investigated.

In order to resolve the issue, what efforts are being taken?

After conducting research on socio-technical and regulatory challenges, the European Parliament's STOA (State of the Art) study (2019) offered legislative alternatives to govern algorithmic transparency and accountability. Improvements in transparency and accountability in algorithmic systems may be achieved via three basic means: In the public sector, decisions based on algorithms must be regulated, monitored, and subjected to formal legal accountability procedures. Additionally, worldwide coordination for algorithmic governance at all levels should be established.

Solutions:

It is possible to have a wide range of evaluation methods even for clearly defined effect scopes (for example, affects on human beings). Quality, consistency, and openness in the review process are essential, as is the skill of those who carry it out. Insufficient training and direction might make researchers feel overwhelmed by the responsibility of considering the long-term consequences. The presence of experts from various fields may assist the assessment of larger impacts.

Vulnerabilities in Cyber Security:

How important the problem is, and why A paper by RAND that examines various viewpoints There are a number of AI-related security concerns that Osoba and Welser (2017) discuss, among other things, new attack approaches based on "data diet vulnerabilities," foreign-deployed artificial intelligence employing network intervention methods, and a larger-scale and more strategic version of the existing enhanced targeting of political messaging on social media are all being investigated. There are other challenges connected to domestic security, such as the increasing use of artificial agents for government monitoring of people (Osoba and Welser, 2017). (e.g., predictive policing algorithms). Their potential to negatively impair basic civil liberties has led to their identification (Couchman. 2019). Because these concerns expose vital infrastructures to serious damages, they pose a serious danger to life and human security and access to resources. Additionally, cyber security flaws represent a serious hazard since they are typically disguised and only discovered after they have already been exploited (after the damage is caused).

How the issue is being dealt:

There are a variety of approaches and methods that may be used to overcome this difficulty. Best practices in data protection and recovery include incorporating human analysts into important decision-making processes, implementing risk management programs, and completing frequent software updates, to name a few examples. Fralick authored a piece titled in 2019 that was published.

Issues Relating To Privacy And Data Security:

How important the problem is, and why CNIL and the ICO both feel that AI presents significant privacy and data protection issues in addition to its impact on other human rights (CNIL, 2017; ICO, 2017). Gardiner (2016a), Informed consent and monitoring are two examples. A new data protection "right to reasonable inferences," which Wachter and Mittelstadt (2019) call the "right to reasonable inferences," should close the accountability gap created by so-called "high risk inferences," which are those that are privacy invasive or reputation damaging, and have low verifiability in the sense of being predictable. Wachter and Mittelstadt are working on a new book that will be published in 2019. It was highlighted in a paper presented at the 38th International Conference of the International Association of Data Protection and Privacy Commissioners in 2016, titled "EDPS, Artificial Intelligence, Robots, Privacy, and Data Protection Background Paper," that increased privacy ramifications and surveillance capabilities were possible. A discussion paper produced by the UK Information Commissioner's Office (ICO) in 2017 said that the ICO was concerned about the misuse of personal data, big data profiling may be intrusive and difficult to comprehend due to the intricacy of the approaches applied in big data research, which makes it difficult to be transparent (ICO 2017).

What's going on and how it's going to be dealt:

The rights of data subjects are only to a limited extent safeguarded by laws regulating privacy and data protection, which provide a bare minimum level of protection to data subjects. It is described as follows in Article 15 of the EU's General Data Protection Regulation that a data subject's right to access and update their personal information includes the following rights: (GDPR). it is highly urged that the possible hazards associated with its usage be made clear (Rigby 2019) MJ Rigby is the author of this article (2019). Ethical considerations in the use of AI in healthcare. developers should "pay particular attention to ethical and legal limits at each level of data processing, We place a high value on knowing where your data comes from so that it may be used and reused in new ways (Vayena, Blasimme& Cohen 2018). There are protocols that enable many parties to collaboratively calculate functions while maintaining the privacy of each party's input that Brundage et al advised for surveillance, such as secure multi-party computing (MPC) (Brundage 2018) Aside from anonymization, privacy warnings, privacy effect analyses, privacy by design, ethical standards, and auditable machine algorithms are among the other methods now being investigated. (As of 2017) The ICO is the government's watchdog for privacy issues (2017) There is a lot of emphasis these days on big data.

Failure to hold wrongdoers accountable:

What To achieve accountability for the development, deployment, and/or use of artificial intelligence systems - risk management as well as detection and mitigation of risks - processes must be put in place that are transparent, can be explained, and can be audited by third-party organizations, according to the arguments of ALTAI. Accountability, responsibility, and openness are the hallmarks of AI. There are two types of accountability in AI: "accountability in AI involves both directing action (by generating belief, decision, and action) and the role of explanation (by putting choices in larger context and by categorizing them along moral standards)" Critics say the "accountability gap" is a more serious issue than first seems, generating difficulties in causation, justice, and recompense. Bartlett & Company (2019) M. Bartlett, Ph.D. (2019). Eliminating the accountability problem in artificial intelligence. Require creators to take responsibility for their work. "Even when a potential harm is found, it can be difficult to ensure accountability for violations of those responsible," report says: "Even when a potential harm is found."

How the issue is being dealt:

"American and European governments today seem to be differing on how to solve present accountability gaps in AI," according to Wachter, Mittelstadt, and Floridi (2017). A 'right to explanation' might be used as a legal tool for AI damage responsibility. Veale, Edwards (2017) Lewis Edwards and Michael Veale are the authors of this paper (2017).

Conclusion:

In the long run, businesses will gain a competitive edge by ensuring that their AI applications comply with ethical standards. Customers are more likely to embrace items that are linked with their values. The European Political Strategy Centre noted that "by respecting the legal right to privacy of users, AI technologies will be more easily accepted by society at large" in light of the growing usage of AI. As a result, ethical concerns may serve as an immediate advantage in the AI market. As a result, regulators and corporations should work together to ensure that AI and autonomous systems defend ethical ideals to the highest degree possible. (EPSC Strategic Notes, supra note 6, at 6.)

Reference:

[1]. EP (2017).

[2]. Theodore D. Munro (2019, January).

[3]. The IEEE P7003 Standard for Algorithmic

[4]. World Intellectual Property Organization (WIPO)

[5]. Frontier Economics was published in 2018. On the Cusp of a Revolution in Economics (2018)

[6]. The UK House of Lords 2018 and the House of Lords Select Committee on Artificial Intelligence

[7]. Munro, D. (2019, January). Governing AI: navigating risks, rewards and uncertainty. Public Policy Forum.

[8]. Prunkl, C. E., Ashurst, C., Anderljung, M., Webb, H., Leike, J., & Dafoe, A. (2021). Institutionalizing ethics in AI through broader impact requirements. Nature Machine Intelligence, 3(2), 104-110.

[9]. Mittelstadt, and Floridi (2017). A 'right to explanation' might be used as a legal tool for AI damage responsibility. Veale, Edwards (2017) Lewis Edwards and Michael Veale are the authors of this paper (2017).

[10]. Bartlett & Company (2019) M. Bartlett, Ph.D. (2019).

[11]. Brundage 2018

[12]. Vayena, Blasimme& Cohen 2018

[13]. Fralick authored a piece titled in 2019 that was published.

[14]. (Rigby 2019

[15]. Article 15 of the EU's General Data Protection Regulation that a data subject's right to access and update their personal information includes the following rights: (GDPR).

[16]. UK Information Commissioner's Office (ICO) in 2017

[17]. Gardiner (2016a),

[18]. Osoba and Welser, 2017).

[19]. Couchman . (2019)

[20]. Meyer, S (2018). Artificial intelligence and the privacy challenge. CPO Magazine . https://www.cpomagazine.com/dat

a-privacy/ artificial- intelligence- and- the- privacy- challenge/ .

[21]. Williams, H (2019). Big brother AI is watching you. IT ProPortal . https://www.itproportal. com/features/big- brother- ai- is- watching- you/ .

[22]. Forbes Insights Team (2019) Rethinking Privacy For The AI Era. https://www.forbes.com/ sites/insights- intelai/2019/03/27/rethinking- privacy- for- the- ai- era/ .

[23]. Dave, P (2018). Fearful of bias, Google blocks gender-based pronouns from new AI tool.

[24]. Reuters . https://www.reuters.com/article/us- alphabet- google- ai- gender/fearful- of- bias- google- blocks- gender- based- pronouns- from- new- ai- tool- idUSKCN1NW0EF .

[25]. the European Parliament's STOA (State of the Art) study (2019)

[26]. EIOPA's Consultative Expert Group on Digital Ethics in Insurance-2021

[27]. GDPR

[28]. Desai and Kroll(2017)

[29]. Cath (2018)

[30]. Privacy International and Article 19 2018; Access Now 2018)

[31]. Principles of Good Governance for AI in the EIS.

[32]. . Rachum-Twaig (2020)

[33]. SSRN

[34]. Artificial Intelligence in Europe for the Year of 2018.