Harnessing AI for due diligence in CBI Programmes. Legal and Ethical Challenges[1]

Jeiel Joseph[2] *and Umut Turksen*[3]

Coventry University

Abstract: Citizenship by Investment (CBI) programmes are defined as 'an exchange of national membership rights for immigrants' financial and human capital' (Gamlen, Kutarna and Monk 2016 pp.6). CBIs represent an innovative and increasingly common mechanism that allows governments to monetise the allure of their countries to migrants, thereby converting intangible assets into financial assets. For applicants, the incentive is a passport, primarily for those coming from troubled regions or those nationalities who encounter visa restrictions of one form or another. Many critics of these CBI programmes have indicated some plausible drawbacks to their practice while further citing that practicing countries have yet to exhaust alternatives before making such a policy move (Williams and Hosein 2019). Substantial integrity and corruption concerns appear to be synonymous with CBI programmes, notwithstanding their regulatory structure (Williams and Hosein 2019). CBI programmes have been criticised by national and international organisations such as the Organisation for Economic Cooperation and Development (OECD), Financial Action Task Force (FATF), the European Commission and the United States Congress. It has been argued that the rapid emergence and growth of such programmes may exacerbate risk of abuse and corruption and raise the possibility of curtailed visa-free access to advanced countries (Xin, El-Ashram and Gold 2015). It is suggested that due diligence can be facilitated and maintained using Artificial Intelligence (AI) tools (e.g., machine learning) in CBI programmes as long as fundamental safeguards are instilled in the development and use of such technology.

Keywords: Citizenship, Investment, Due Diligence, Artificial Intelligence

[1] Research for this paper received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 101022004.

[2] PhD Candidate at the Centre for Financial Integrity, Coventry University. LLB & LLM (Kingston University, UK) Email: josephj12@uni.coventry.ac.uk.

[3] Professor in Law at the Centre for Financial and Corporate Integrity, Coventry University. PhD (UWE, UK); LLM (UWE, UK). Email: umut.turksen@coventry.ac.uk.

1. Citizenship by Investment Programmes

CBI is the process by which a government grants citizenship rights to an applicant in exchange for a financial investment or other direct investment into the host country. CBI programmes are unique as they do not fit into traditional models of naturalisation and citizenship. CBI programmes are an expedited form of naturalisation, and their use has been considered by many industry protagonists to be a unique access to second citizenship, rather than by birth right acquisition, be it by descent (*jus sanguinis*) or by birth in the territory (*jus soli*) (European Union Institute 2017). Unlike international trade and finance, which are governed by the World Trade Organisation (WTO) and International Monetary Fund (IMF), the CBI industry has no global regime to set binding policies or due diligence standards on applicants (Gamblen 2010). Instead, each individual state experiment with investment migration policies to further their own interests.

While some of the risks posed by CBI programmes emanate from malfeasant applicants (external factors), there is also the possibility that CBI programmes may be exploited by corrupt officials in the CBI host countries. For example, in 2020, the Cypriot CBI programme was terminated after leaked government documents revealed (Kambas 2021) that Cypriot passports were being sold to convicted criminals, money launderers, and to individuals entrusted with prominent public functions in their respective home countries, known as 'politically exposed persons' (PEPs) at higher risks of corruption. European CBIs, such as those offered by Malta and previously by Cyprus, have been bearing most of the criticism by financial regulatory organisations regarding their due diligence processes (European Commission 2019). The European Union Commission (EC) has further published reports specifically addressing 'Investor Citizenship and Residence Programmes' in the EU (European Commission 2019). The EC expressed concerns over the implications and risks that CBIs might pose to security and facilitating financial crime, including money laundering and other illicit financial flows on a global scale. It should be noted however such risks arise not only within CBI programmes but also in other settlement by investment (e.g. golden visa programmes which are offered by many states including Germany, Ireland, United States of America, United Kingdom, Portugal) and non-investment schemes for acquiring citizenship.

Given the speed of which a person acquires citizenship under CBIs, it is arguable whether these risks emanating from the practice of CBI are sufficiently addressed by current '*modus operandi*' of due diligence practices therein. Furthermore, there is no internationally agreed due diligence standards in CBI programmes which leads to the consensus that such programmes may be exploited by criminals particularly for money laundering purposes

(OECD 2019). Most CBI host countries have adopted recommendations of the FATF and OECD as part of their due diligence practices to a certain degree. While the Investment Migration Council (IMC) formed a specific due diligence working group exploring the potential for the creation of minimum due diligence standards in CBI programmes (Oxford Analytical 2020), there is no evidence of CBIs adopting the IMC's recommended minimum due diligence standards.

This article is a novel study which aims to identify legal and ethical implications of using AI for enhancing due diligence practices in CBIs. Firstly, it explains CBIs and provides a comparative analysis of due diligence practices therein. It then considers what type of AI may be employed in enhancing due diligence practices in CBIs. In doing so, it outlines several fundamental ethical and legal issues which may arise when AI based decision making process are engaged. It then offers a critical analysis of ethical and legal requirements which shall be observed in creating and utilising AI technology. Finally, the paper puts forward several recommendations which may serve as safeguards in using AI for complementing due diligence practices.

Due Diligence in CBI

Due diligence in CBIs is conducted by licensed agents, citizenship by investment units (CIUs) and third-party service providers. Therefore, any application of AI and its implications for human rights and ethics will mainly be faced by these key stakeholders. In this *modus operandi*, it is the role of licensed agents to conduct the initial screening of the applicant and thereafter present their application to government CIUs. As such, agents have the first opportunity to identify, screen and reject candidates that fail to meet the respective CBI application criteria. Whether or not agents make an adequate initial decision depends in part on the level and quality of due diligence they conduct but is also potentially influenced by fees which agents earn in processing applications. It is not difficult to imagine that in an unregulated industry, agents may be pressured by applicants to expedite or even turn a blind eye to information deemed to pose a medium or high risk. When an application for CBI is undertaken which is deemed to be 'high risk', government CIUs may also be required to perform enhanced due diligence checks on clients, via third party due diligence providers, after the 'on-boarding' stage conducted by agents. The analysis of the CBIs which are currently active in countries such as Antigua and Barbuda, Dominica, Cyprus, Malta, St Kitts and Nevis, St Lucia, Grenada, Vanuatu reveals how current due diligence processes are typically multi-tiered and facilitated by the CIU using a hierarchical framework. The due diligence protocol within these CBIs operates as follows:

Stages	Process	Actor	Actions
Stage 1	KYC processes and initial screening	Agent	Confirm applicants' identity Search databases for instances of sanctions or presence on international criminal watchlists Initial assessment of the applicants' source of funds
Application submitted to government			
Stage 2	International and National Intelligence and law enforcement	Government CIU	Searching domestic intelligence, foreign partners' intelligence, local law enforcement. National databases Outstanding warrants Suspicion of international criminal activity Check for criminal record Check for failed visa applications and reasons for rejection. Checking with Interpol and other agencies for information on the applicant.
	Due Diligence from third party provider	Third party due diligence providers	Searching international intelligence, personal interviews, online databases and physical archive access: Searches of litigation records; PEP/ political exposure; regulatory issues Checks on trustworthiness and reputation Adverse media assessment Validation of primary documents Checks on disclosed and non-disclosed businesses.
Applicant risk profile created			
Stage 3	Creation of risk assessment		Government CIU

Table 1-CICIP due diligence process

There are sufficient similarities in the due diligence processes in programmes, which include the mechanisms used for collection, and the multilayer process that includes the work of agents, CIUs and third-party providers (European Parliament 2021). These commonalities should serve as a base for setting AI facilitated minimum standards for these due diligence actors. It is opined in this contribution, that CBI due diligence can benefit from the introduction of AI only if fundamental rights such as privacy (Article 8 of the European Convention on Human Rights 1950; Article 8 and 12 Universal Declaration of Human Rights 1948 and Article 17 of International Covenant on Civil and Political Rights 1966), equality and non-discrimination (Article 14 of the European Convention on Human Rights 1950; Article 1 and 2 of the Universal Declaration of Human Rights 1948) (as will be seen) are maintained consistently by all CBI stakeholders.

The OECD has published the 'Due Diligence Guidance for Responsible Business Conduct' which provides practical support on the implementation of the OECD Guidelines for providing plain-language explanations of its due diligence recommendations and associated provisions (OECD 2018). The FATF 40+ Recommendations, on the other hand, are recognised as the global anti-money laundering (AML) and counter financing of terrorism (CFT) standards, which are followed by CBI practicing states (FATF 2012). Virtually all AML regulations require that financial institutions (and other key obliged entities) monitor and report any suspicious transaction. CBI stakeholders, in compliance with the AML rules, also need to ensure that applicants are not listed on international sanctions lists or blacklists as it is prohibited to do business with such entities. A key element in an effective due diligence process is to be able to quickly identify applicants in consideration of AML/CFT regulations and moreover comply with international minimum standards so that the integrity of the CBI and fundamental rights of the applicants are upheld.

Identification and know your customer

The identification and know your customer (KYC) due diligence processes in CBIs have evolved from simple formality into a detailed requirement supervised by national authorities i.e., citizenship by investment units (CIUs). The FATF provides the international standards for KYC and best practices for all CBIs and their stakeholders which include the following actions:

Identify the customer and verify that customer's identity using reliable, independent source documents, data, or information.

Identify the 'beneficial owner', verify the beneficial owner's identity, and understand the ownership and control structure of the customer; and

Understand and obtain information on the purpose and intended nature of the business relationship.

In the current *modus operandi*, these requirements must be met by each stakeholder before they establish a financial (e.g., CBI) relationship with a new applicant. Thus, if one applicant works (or intends to work) simultaneously with more than one agent, the KYC process for that applicant will be repeated. Although each agent is responsible for their own KYC process and must conduct due diligence independently of other agents, a core portion of KYC due diligence is a routine process that is carried out in parallel by all agents that work with the same applicant. As a consequence, costly tasks are carried out repeatedly and simultaneously whenever an applicant works with two or more agents.

KYC due diligence in this early stage of the application, should consider the legitimacy behind the investment by authenticating the applicant's wealth, assets, funds, and business records. Applicants must fulfil a source of wealth declaration not only in line with national law but also in line with the guidelines and regulations set out by the OECD and FATF. Verification of an applicant's source of wealth should be a common practice across all CBI programmes. Agents should also be prepared to undertake a broader examination of an applicant's sources of wealth, as illegal activities may be concealed in assets that are not used for the application but would ultimately disqualify the applicant. Consideration should be given to include this broader source of wealth perspective in minimum due diligence standards. The EU's 5th AML Directive stipulates that the aforementioned process should be done by using electronic identification (European Union 2018).

Strong due diligence in the KYC 'on-boarding' process will create a structured basis for the facilitation of minimum due diligence standards within the CBI industry. In this premise, licenced agents must perform independent verification of the applicant's identity, through address-corroboration using online database tools. It is the role of an agent to collect and verify documentation and data concerning the applicant's identity throughout the 'on-boarding' process. The agent must make sure that the applicant is one of outstanding character, hold no criminal record, own a valid passport, and birth certificate. Moreover, agents need to verify the authenticity of the information that clients provide to ensure that they are who they claim to be.

AML Compliance

A key aspect of the CBI due diligence process is compliance with minimum AML standards provided by the OECD and the FAFT, and for EU entities, the EU's AML Directives. Governments conducting these programmes must have implemented AML/CFT standards into their national laws. Minimum AML/CFT compliance standards should include clearance from local police authorities from countries where applicants reside (Oxford Analytical 2020). CBI actors should do this by checking police databases such as INTERPOL to ensure there are no outstanding warrants or other criminal proceedings against the applicants, their businesses and/or close family members and associates.

Regarding financial crime in Europe, the EU 5th AML Directive on the prevention of the use of financial systems for the purposes of money laundering or terrorist financing is applied holistically across all EU Member States (European Union Fifth AML Directive 2018). All other CBI stakeholders outside of the EU are obligated by the FATF 40+ Recommendations. In CBI programmes, money laundering and corruption concerns are the primary justification for verifying an applicant's source of wealth, and even greater justification for compliance with international legal instruments (e.g. the United Nations Convention against Corruption, 2003).

Essentially, to mitigate potential AML/CFT risks, minimum compliance standards would require all agents (who perform the initial on-boarding of clients) to register with the relevant national local authority for AML compliance supervision, as there is no proof that this is currently being done with specific regards to agents. Moreover, compliance standards would encourage agents to notify these national compliance institutions when an applicant seeks citizenship through investment so that they can be made aware and apply the appropriate level of AML/CFT due diligence using the appropriate standards.

2. Minimum due diligence standards facilitated by AI

This section articulates a minimum due diligence standard for CBI and can be used as a foundation for the process of on-going improvement, which would be facilitated by stakeholders using AI tools such as Machine Learning (ML) and Block Chain Ledgers (BCL). Before explaining how AI can enhance due diligence, however, it is important to define what is meant by AI and what type of AI may be suitable for due diligence in CBI programmes.

What is AI?

Having captured the public's imagination since the term was first coined by McCarthy in 1955 (McCarthy 1955), AI does not have a universally agreed definition. A number of commentators asserted that AI refers to 'machines or computers that mimic cognitive functions that humans associate with the human mind, such as learning and problem solving' (Russell and Norvig 2009). Thus it is envisaged that the future of this technology will be cognitive, not "artificial" (Kelly 2016). This approach derives from the desire to innovate technical capability in par with human intelligence whereby AI is articulated as 'the biopsychological potential to process information… to solve problems or create products that are of value in a culture' (Gardener 1999, pp. 33-34).

AI has been categorised into four types of activity or processes, namely: thinking humanly, acting humanly, thinking rationally, and acting rationally (Russel, Norvig and Davis 2016). Under the thinking humanly category, AI has thus also been defined as 'the exciting new effort to make computers think' (Haugeland 1985). In essence, this type of approach to AI whereby it is compared to humans is not very different from the definition of AI under the acting humanly category – 'the art of creating machines that perform functions that require intelligence when performed by people' (Kurzweil 1990, p. 21). It is however not completely accurate to define the function of the AI as 'human thinking' because unlike the human cognition and decision making, all AI systems rely on three essential components: computing capability (hardware), developing advanced algorithms (software), and access to relevant and reliable data to exploit. Currently, all these components are provided by people thus, an AI system is also reliant on human input. The second category of 'the thinking rationally' defines AI as 'the study of the computations that make it possible to perceive, reason, and act' (Charniak and McDermott 1985, pp. 2) while the acting rationally category defines AI as 'the study of the design of intelligent agents' (Poole Mackworth and Goebel 1998, pp. 1-2).

While the term AI has existed for over 50 years, the access to and convergence of vast datasets (a common feature in CBI application process), powerful hardware and advanced algorithms have made application of AI in various contexts and in high-functioning robotics a reality only in the last decade. Like its definitional categories, based on its sophistication and capabilities, AI has also been categorised in terms of its actual and 'anticipated' evolutionary use. Accordingly, AI is categorised by first, second and third generations. The first generation of AI which is commonly available in many devices which we use daily mostly deals with finite number of tasks thus referred to as 'artificial narrow intelligence' (Poole Mackworth and Goebel 1998). Voice and face recognition, self-driving or autonomous vehicles are some of the examples of the first-generation AI systems. AI is also used to support several businesses needs *inter alia*, process automation, cognitive insight, and cognitive engagement (Davenport and Ronanki 2018).

Process automation is the use of technology to automate digital and physical business processes to transition from one task to the next sequentially with minimal human intervention. Cognitive insight is the use of algorithms to detect patterns in vast volumes of data and interpret their meaning which can be employed for example, to re-evaluate thoughts and beliefs in order to make thoughtful conclusions (Camp 2017) and/or automated decision making. Cognitive engagement (Kelly 2016) refers to AI embedded systems such as chatbots and intelligent agents that are used to support decision-making, deliver highly relevant information, and optimise the available attention to avoid missing key developments (Kelly 2016). Cognitive AI systems are probabilistic whereby they not only generate answers to mathematical problems but also hypotheses, reasoned arguments, and recommendations about more complex—and meaningful—bodies of data. As is the case for almost all AI systems, in the context of AI in CBI programmes, it is essential that the data available to decision makers is reliable. Accordingly, if the data-sets available to CBI programmes are fragmented or locked in proprietary 'application programming interface' solutions controlled by supplier companies, there would be additional challenges to the quality of decision making and effectiveness of the system (UK Ministry of Defence 2018).

Despite these potential challenges, it is expected that there will be the second-generation of AI in the coming years, also referred to as 'artificial general intelligence', which would be able to reason, plan, and solve problems autonomously for tasks they were never designed for. Given the political and legal initiatives surrounding the use of such technology in the context of defence systems, it is not unreasonable to think that the second-generation AI is either ready and operational or is on the brink of being operational. The second-generation AI will be based on non-deterministic systems[4] whereby the system will be able to explain why the system made a particular decision.

If the AI technology advances as anticipated, there would be the third generation of AI, conned as 'artificial super intelligence', which would consist of self-aware and conscious systems that could, to a certain extent, make human thinking and decision making redundant. If materialised, such a technology, would have very different characteristics from those attributed to AI as we know today which inevitably would pose several technological, scientific, legal, ethical and societal challenges and opportunities, with different requirements for governance, policy, and enforcement. It is envisaged

[4] Non-deterministic systems are characterised as those where very small changes to inputs can produce very large changes to outputs. Non-deterministic systems are associated with unpredictability. UK, Ministry of Defence, Joint Concept Note 1/18, p. 11.

that the future of AI is going to run faster; operate on low costs and power demands; and offer broader application (UK Ministry of Defence 2018).

There is now growing literature on the ethics and regulation of AI, particularly in the context of its use by government agencies (Ranchordas 2021). New technologies and innovation create, by nature, regulatory challenges, particularly in the context of traditional and reactive regulatory frameworks, which include CBI programme due diligence framework. Regulating AI is particularly challenging, not just due to the speed of the changes at stake, but because of their pervasiveness and the foreseeability of future AI applications (Ranchordas 2021). It is unsurprising, therefore, that significant concerns have been raised in relation to the ethical use of AI, in this context, harnessing AI to facilitate due diligence in CBI programmes.

The proposed EU AI Regulation provides a general and encompassing concept of AI and defines AI system as a software '…that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with…' (Article 3, European Commission 2021b) Furthermore, it lists various categories of AI based on the purpose and risks they may pose when deployed (European Commission 2021b).

Potential uses of AI in CBI programmes

Whilst there are many different AI tools in use globally, some of the most significant and controversial ones can be divided into three main types: a) risk assessment tools; b) real-time technology; c) compliance assistance technology. The first two types can be broadly characterised as systems inducing negative incentives for compliance, or anti- fraud mechanisms; the third as offering positive incentives for compliance (e.g. for tax compliance), or compliance-enhancing mechanisms (De la Feria and Ruiz 2022). Risk assessment analytical tools have spread throughout the world (OECD 2014) some of which focus on identification of high-risk applications, including through big data sourcing and profiling, such as the Italian's FALCO system, or the Dutch XENON robot (Ehrke-Rabel 2019). Other systems are aimed at improving the effectiveness of financial audits, known as computer-assisted audit tools and techniques (CAATTs), which have been implemented by several countries, including Australia, Finland, Germany, Indonesia and the US (Darono and Ardianto 2016).

The primary argument for the implementation of AI in CBI is due to the fact that money laundering and financial fraud techniques practiced by malfeasant applicants are complex and constantly evolve. As such, new and promising techniques should be developed and applied in CBI programmes, to assist in identifying and flagging suspicious behaviours. In this premise, there is currently no observable framework or formal set of recommendations on what should be regarded as suspicious interactions between applicants and agents in CBI. Accordingly, ML (in the form of a risk assessment tools) can help to realise certain deviations from typical patterns which may trigger further probing to look at the significance of specific events or transactions.

Monitoring these complex transactional relationships in the *modus operandi* of CBI due diligence can be slow, laborious, and costly for both the agents and CIUs. Trying to manually deduce patterns from malfeasant behaviours by sifting through large pools of unstructured data, often in different formats and languages, and dealing with a possibility of a high volume of false positive results can consume extensive human resources, and not get the agent or CIU any closer to being assured that they are dealing with a legitimate applicant. As the recent leaks such as Panama and Pandora Papers have demonstrated, it is not only the volume and type of data which can overwhelm the authorities but also the sheer number of people, companies, business operations and assets that are scattered across the globe.

Industry antagonists may argue that by using conventional automation and data mining techniques, as opposed to modern AI techniques, for facilitation of minimum standards in identification and compliance, would be cheaper and more effective in the current regulatory climate and in consideration of the lack of AI readiness or capacity in some countries. Even if a country was prepared to adopt a conventional AI tool for due diligence in CBI, such system may be complicated by the fact that there is currently very little organised historical data available on what types of activities to look for, and what types of transactions should trigger alerts. With conventional data mining methods, there is still no clear benefit in consideration of accountability or transparency across the CBI industry.

AI tools are also fuelling innovation by transforming the way organisations view data analytics (European Commission 2016). Instead of giving computers rules to solve problems, businesses are granting machines access to data and asking them questions, so that they can learn and "think" of solutions for themselves (H20.ai 2017). These technologies are ideally suited for facilitating a minimum due diligence standard, including but not limited to, 360° KYC by integrating information from various sources, studying the typical money transfer patterns in consideration of AML compliance, differentiate in 'real time' between usual and suspicious behaviours boosting performance, multilateral communication of the revocation of citizenship of applicants.

AI solutions in CBI can, for example, find patterns that traditional rule-based tools are not able to detect and can continuously learn and adapt in response to changing applicant behaviours, programme environments and regulations (H20.ai 2017). Weight must also be placed on the fact that while large and medium-sized agents and CIUs can hire armies of experienced compliance officers, small-sized equivalents cannot afford to do the same. With a limited number of officers and the importance of successful transactions, smaller firms need in both cases - to work smartly to detect circumstances which fall below the suggested minimum due diligence standard threshold, and in doing so with minimal false positive or false negative. In this regard, and to reiterate, AML regulations require that financial institutions (working alongside CBI stakeholders) monitor, investigate, and report any suspicious transaction. Agents in administration of AML compliance, before applying to the CIU, need to ensure that the applicants are not listed on criminal blacklists as they are thereby prohibited to do business with them and could breach AML standards.

AI tools such as ML, can also be used to enhance the productivity and competitiveness of CBI stakeholders by fostering transparency, innovation and reducing the costs of various due diligence activities. Thus, the existing agents would need to have advanced digital skills and literacy to take advantage of such AI technology in the workplace. Developing countries such as those in the Caribbean who practice CBI, in particular, face a range of challenges that inhibit AI advancement in several areas. These include weak implementation capacity, limited financing related to the lack of economic scale, and low levels of regional collaboration on common platforms, regulation and policy, and standards (Ram 2021). Ram also indicated that efforts are needed to improve regulatory frameworks, cross-border data flows, security, consumer protection, and, importantly, increase the availability and affordability of broadband access for vulnerable populations (Ram 2021).

Whilst this may not be a problem for a CBI in a developed country, it is observed that only a small percentage of the workforce has formal training in advanced ML tools in the Caribbean (Ram 2021). Thus, Governments in the Caribbean region should provide sufficient funding and support to ensure that CBI agents have the necessary tools, skills, and resources to achieve the tangible benefits from the aforementioned digital technologies. Governments also ought to prioritise establishing the legal and regulatory frameworks that foster the use of AI tools by agents in conducting the initial due diligence process.

Implementation of AI tools at a CIU level can help improve transparency, accountability, efficiency and competitiveness in the industry. Such modernisation involves technologies becoming progressively embedded in CIU activities to improve services and efficiency in delivering sound decisions on applications. Consequently, as third-party due diligence providers adopt modern technologies in conducting their due diligence processes, CIU authorities must also have adequate skills and knowledge to utilise and understand the technologies adopted by third party providers. Moreover, senior officials in CIUs need to understand emerging technologies and the novel technological roles in conducting due diligence on applicants. Unlike in the EU Member States, governments in the Caribbean do not have specific strategies to attract, create or retain CIU employees who are skilled in digital technologies such as in ML. This highlights the need for coherent and coordinated policy actions to develop skills and training required to support a data-driven CIU. To grasp the new opportunities that AI such as ML or block chains are creating in CBI due diligence, stakeholders, should obtain the relevant digital skills and literacy to make meaningful use of these technologies. Thus, there is a need for targeted programmes on a national and regional level to train stakeholders in the specific use cases of AI in minimum due diligence standards.

3. Legality and Ethical Issues

From the perspectives of law and ethics, it is observed that the current focus on AI is based on impressive progress being made in the technical fields of ML and deep neural networks, such as performances from banks' customer service robots to AI technologies like natural language processing exhibiting serious potentials to improve the experience of stakeholders through interpretation of their voice, email, and even unstructured requests. Another example includes the KYC onboarding process being shortened significantly due to AI tools using document text extraction and facial recognition systems being used to access secure information and accounts. There have been concerns regarding the legality and ethical soundness of these AI applications (Raphaël 2022).

Whilst, AI technology possesses the potential to correct human biases if it is well-designed (Sunstein 2021), there is now strong evidence that many algorithms not only entrench the biases of its designers, but augment them (Mayson 2019). AI is often trained to identify correlations between characteristics and outcomes, using those correlations and/or patterns to predict future outcomes (Kleinberg 2018). The problem is that correlation is not causation and inferring causation from mere correlation can often lead to discrimination of specific groups, such as women or racial minorities (Criado-Perez 2019). In CBI due diligence, risk assessments are also particularly susceptible to these profiling problems which could be exaggerated with the introduction of a novel AI system. The potential repercussions of such a profiling are illustrated in a recent Dutch AI scandal (Berg 2021). Over the last decade, more than 26,000 Dutch families were wrongly accused of fraud, after being singled out by AI designed to detect large-scale fraud; more than half had an immigrant or vulnerable background. This problem may arise if and when CBI applicants in a hypothetical AI due diligence system are singled out as high-net-worth individuals which subsequently may produce false positives due to the potential of profiling. Article 29 Working Party, the predecessor to the European Data Protection Board, addressed, as early as in 2011, the need to balance privacy and data protection rights against risk mitigation objectives (European Commission Working Party 2018). Eventually, in 2017, the European Council called for a 'sense of urgency to address emerging trends' including 'issues such as artificial intelligence ..., while at the same time ensuring a high level of data protection, digital rights and ethical standards' (European Council 2017). In its 2019 conclusions on the coordinated plan on the development and use of artificial intelligence made in Europe (European Council 2019), the Council further highlighted the importance of ensuring that European citizens' rights are fully respected and called for a review of the existing relevant legislation to make it fit for purpose for the new opportunities and challenges raised by AI. The European Council has also called for a clear determination of the AI applications that should be considered high-risk (European Council 2020). In this regard, the EU's General Data Protection Regulation (GDPR) has been regarded as one of the most important instruments for the regulation of AI (European Commission 2016). It features a risk-based approach, which has been framed as a scalable approach to compliance with existing data protection obligations and requirements (European Commission 2016).

The EU Commission in 2021 published their proposal for laying down harmonised rules on Artificial Intelligence, with the intention of putting forward legislation for a coordinated approach on the human rights and ethical implications of AI (European Commission 2021b). This is the first legislative framework on AI that has been put forward by the EU and has the potential to "set the tone" for other jurisdictions (including CBI practicing states outside the EU) as they also look to put some regulatory parameters around the development and use of AI. Notably, this proposed AI Regulation is not only novel, but it is a comprehensive framework as other legislation in the EU merely touch the topic of AI and do not holistically introduce 'risk-management' considerations for EU AI systems. Just like the GDPR, the proposed AI regulations is also underpinned by a risk-based approach. In the first case, the point is to use risk and risk management tools as a means to better comply with the GDPR. In the second, the point is to determine which AI systems themselves should be regulated.

The proposed EU AI Regulation requires a risk-based approach to the use of AI technology whereby high-risk AI systems would be subjected to stricter safeguards.[5] Article 5 of the proposed AI Regulation deems certain types of social scoring and biometric surveillance to be an "unacceptable" risk to privacy, non-discrimination, and other related human rights, thus bans such AI systems completely (Section 5 of the Explanatory Memorandum, European Commission 2021b). Public authorities are prohibited from scoring people's "trustworthiness" in one aspect of their lives (e.g. their ability to repay debt) to justify "detrimental or unfavourable treatment" in another, unrelated context (e.g. denying them the right to travel).[6] In the opinion of the authors of this paper, the current proposal to ban some types of "trustworthiness" scoring over a "certain period of time" is vague and impossible to implement meaningfully (Article 5, European Commission 2021b). Instead, the regulation should prohibit any type of behavioural scoring that unduly restricts or has a negative impact on fundamental human rights such as privacy and non-discrimination. In application to CBI AI, the hypothetical scoring systems that would try to predict whether applicants are a fraud risk based on KYC records or serve as a pretext for acceptance or denial of an application, should be banned if it conflicts with an applicant's fundamental human rights, including privacy and non-discrimination.

The EU's proposed AI Regulation requires each AI system to be classified in terms of the risks such AI may pose to society. The category of the AI system proposed for due diligence in CBIs would be categorised as a "high-risk" AI system as it would handle and analyse personal information which would in turn contribute towards determining whether the CBI applicants would be entitled to citizenship. Importantly, the proposed AI Regulation designates an expansive list of AI systems as "high-risk" that would require extra safeguards to deploy. More specifically, these systems include those used to

[5] The proposed AI Regulation contains specific rules for AI systems that create a high risk to the health and safety or fundamental rights of natural persons. High-risk AI systems are permitted on the European market subject to compliance with certain mandatory requirements and an ex-ante conformity assessment. The classification of an AI system as high-risk is based on the intended purpose of the AI system, in line with existing product safety legislation. Therefore, the classification as high-risk does not only depend on the function performed by the AI system, but also on the specific purpose and modalities for which that system is used. The European Commission describes these systems as "limited risk" systems, but this description is not explicit in the regulation. European Commission, "New rules for Artificial Intelligence – Questions and Answers," April 21, 2021, <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683>, accessed 18 April 2022.

[6] Ibid.

identify and categorise people based on their biometric data, such as facilitating a minimum KYC due diligence standard in CBI programmes (European Commission 2021b). The proposed AI Regulation introduces provisions which require "high-risk" systems to adhere to a series of risk mitigation requirements which outline the types of information that should be kept and disclosed about a system, safeguards against bias and error, and measures to ensure human oversize, accuracy, robustness and cybersecurity (European Commission 2021b). The proposed AI Regulation also covers limited-risk AI system,[7]which includes "biometric categorisation," emotion recognition, and deep fake systems (Gregory 2021). These do not require the same oversight as "high-risk" systems. Moreover, low risk AI systems are all other systems not covered by the regulations requirements and safeguards (Gregory 2021).

AI use cases in facilitating minimum standards would have to meet certain "high-risk" requirements under this proposed regulation, which could be deemed as onerous. Therefore, as the use of AI in CBIs offers many opportunities, it offers, equally, many challenges. The vast amount of data available to CBI stakeholders empowers advanced decision-making, but in tandem also raises questions pertaining to the quality of the data sets and how these are utilised. Provisions of the proposed AI Regulation require that the data sets used in creating an AI system must be free of errors (European Commission 2021). The AI Regulation also sets harmonised rules for the development, placement on the market and use of AI systems in the EU following a proportionate risk-based approach.[8] It can be recommended, therefore, that the placement of AI facilitating minimum due diligence standards in the CBI industry, shall also take a proportionate risk-based approach. It is important that an AI system in CBI programmes follows predictable, proportionate, and clear obligations, which are also placed on providers and users of those systems to ensure safety and respect of existing legislation, protecting fundamental rights throughout the whole AI systems' lifecycle.[9]

This is a model which should be followed by CBIs for all intents and purposes. The legal requirements for a high-risk CBI AI system, in relation to data and data governance, documentation and record keeping, transparency, human oversight, robustness, accuracy and security, must be clear. The proposed AI Regulation by the EU suggests that AI facilitators (e.g., CBI stakeholders) refer to the Ethics Guidelines of the High-level expert group

[7] The European Commission describes these systems as "limited risk" systems, but this description is not explicit in the regulation. European Commission, "New rules for Artificial Intelligence – Questions and Answers," 21 April 2021, <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683>, accessed 18.04.2022.

[8] Ibid.

[9] Ibid.

on artificial intelligence - HLEG (European Commission 2019). Furthermore, the proposed EU's AI regulation mandates that human rights impact assessments be performed throughout the lifecycle of the AI system. During the conceptualisation and implementation phases of the CBI AI system, these impact assessments could help to expose any potential human rights risks that may otherwise elude existing CBI programme risk management processes.

4. Recommendations

While the due diligence and risk assessment protocols and standards exercised by stakeholders in CBIs are often informed by well-established rules (e.g. FATF AML Recommendations), the use AI to enhance these practices is a new and novel concept which has not so far been regulated. If CBI programmes are to be managed by the use of AI technologies in the future, the legal framework as put forward by the EU shall be followed. The standards and safeguards provided by the EU's proposed AI Regulation mandate that the rule of law by design, human rights by design and ethics by design must be observed at the creation stage of the AI. In addition, regular human rights impact assessments throughout the life cycle of the system shall be conducted. These fundamental benchmarks are important for the potential use of AI in CBIs because, during the design and testing phases of the CBI AI system such assessments could potentially expose human rights risks that may otherwise elude existing risk management processes, such as bias testing or data protection assessments.

Accordingly, the following safeguarding standards may be put forward for the use of AI in different stages in CBIs. As such, in the Pre-Deployment stage, it is recommended firstly that governments practicing CBI programmes using AI conduct and publish privacy and non-discrimination impact assessments prior to deploying or procuring the "high-risk" AI system. Governments should thereafter address issues of AI readiness and other obstacles that stakeholders with low digital literacy or nations with unreliable internet access might face, this should be conducted throughout the lifecycle of the AI system. CBI stakeholders should also be provided opportunities to participate in the procurement, design, or relevant modification processes in the pre-deployment stage of the AI system. This can be done through public hearings, comment procedures, consultations and testing with other directly affected stakeholders, such as licensed agents and third-party party due diligence providers. Finally, governments should encourage a multilateral approach of the relevant CBI stakeholders. This will assist in providing equal opportunities to participate in procurement and relevant modification processes through multilateral stakeholder hearings including notice, comment procedures and consultations.

Once a system is deployed, governments should require CIUs to publicly disclose the results of bias audits and subsequent corrective action. Moreover, the creation of an independent oversight body at the national level that is responsible for conducting regulatory inspections is recommended at this post deployment stage. It is mandatory that regulatory inspections that assess the privacy impact of "high-risk" systems in CBI, such as the training, resources, and protections provided to stakeholders operating or overseeing these systems be conducted (Ada Lovelace Institute 2020). CIUs can also establish a flagging mechanism that gives them the right to request that an independent oversight body investigate an AI system within the jurisdiction for compliance with human rights standards. In consideration of a deterrence mechanism, governments should require licensed agents or users of the system who consistently fail bias audits or regulatory inspections to cease providing or using the system. Last but not least, CIUs should ensure that internal staff have the resources to conduct internal CIU human rights oversight to perform inspections and investigations.

Finally, in consideration of General Oversight (Pre and Post deployment), CBI host states must establish mechanisms to appeal decisions facilitated by an automated system. Moreover, they should also require agents and CIUs using these systems to publish information about their use of "high-risk" AI systems, including their name, the start and end dates of use, and the specific purpose for which they are using these systems (e.g., the specific applicant for which they are using the system, and the specific tasks assigned to the system in relation to that applicant). These CBI host states should necessitate the development of whistle-blower mechanisms and other anti-retaliation safeguards that protect an applicant when they override or otherwise challenge an automated decision. Administratively, CIUs should not leverage the introduction of automated systems to justify reductions in CIU staff as this will end up hindering their ability to re-train staff to operate and oversee these systems. Finally, the imposition of fines and other penalties for non-compliance with human rights impact assessments and other risk mitigation requirements, should be mandated for stakeholders in consideration of the nature and severity of the non-compliance.

When taking into consideration the maintenance of these safe-guards and protocols, CIUs and agents would also need to undergo administrative retraining to effectively work in collaboration with the AI system. The continued development of privacy rights in consideration of the sale of citizenship is required as the industry is dynamic and faces due diligence risks related to KYC and AML compliance. The aforementioned recommendations suggest a specific 'use case' for AI in CBI programmes. This approach is essential to mitigate the potential violation of a stakeholder's fundamental rights such as privacy. Importantly, these recommended standards are transferrable to other areas of practice where AI facilitated due diligence on people and companies may be employed.

5. Conclusion

Granting of citizenship for money is contentious even without the associated risks (e.g. security, crime, corruption) posed by applicants. When coupled with such risks, it becomes even more important to instil integrity and safeguards in CBI programmes. This article highlighted the need for standardised and better due diligence practices in CBI programmes. In doing so, it offered a critical analysis of if and how AI technology can complement the decision-making protocols. Furthermore, this critique identified actual and potential legal and ethical problems in the use of AI for decision making. Finally, a number of safeguards and recommendations have been put forward to mitigate these risks posed by the use of AI technology in due diligence practices.

As technology develops at a lightning speed and the laws continuously tries to catch up with it, this article emphasises the need for rule of law by design, human rights by design and ethics by design principles in developing any technology. Without such considerations, the benefits and common good deriving from such new technology are likely to be limited.

Bibliography

ADA Lovelace Institute. 2020. "Examining the Black Box: Tools for Assessing Algorithmic Systems." www.adalovelaceinstitute.org. 2020. https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems.

Antigua and Barbuda Citizenship by Investment Act. 2013.

Baker, Raymond W. 2005. *Capitalism's Achilles Heel: Dirty Money and How to Renew the Free-Market System.* Hoboken, N.J.: John Wiley & Sons.

Charniak, Eugene, and Drew Mcdermott. 1991. *Introduction to Artificial Intelligence.* Reading, Mass.: Addison-Wesley.

Commonwealth of Dominica Citizenship by Investment. 2013.

Council of the European Union. 2019. "EUROPEAN UNION INSTRUMENTS in the FIELD of CRIMINAL LAW and RELATED TEXTS." https://

www.consilium.europa.eu/media/41918/eu-instruments-in-the-field-of-criminal-law-and-related-texts_december-2019.pdf.

European Commission. 2021. "Press Corner." European Commission - European Commission. April 21, 2021. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683.

European Commission. 2016. "REPORT from the COMMISSION to the EUROPEAN PARLIAMENT, the COUNCIL, the EUROPEAN ECONOMIC and SOCIAL COMMITTEE and the COMMITTEE of the REGIONS." https://ec.europa.eu/info/sites/default/files/com_2019_12_final_report.pdf.

———. 2019. "Ethics Guidelines for Trustworthy AI."

———. 2021. "Council Regulation (EC) 2021/0106.

———. 2021b. "EUR-Lex - 52021PC0206 - EN - EUR-Lex." Europa.eu. 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

European Parliament. 2019. "Texts Adopted - Report on Financial Crimes, Tax Evasion and Tax Avoidance - Tuesday, 26 March 2019." Www.europarl.europa.eu. 2019. https://www.europarl.europa.eu/doceo/document/TA-8-2019-0240_EN.html.

European Union. 2018. "Fifth AML Directive."

FATF. 2012. "Documents - Financial Action Task Force (FATF)." Fatf-Gafi.org. 2012. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

———. 2013a. "'Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals.'" Www.fatf-Gafi.org. 2013. http://www.fatf-gafi.org/publications/methodsandtrends/documents/mltfvulnerabilities-legal-professionals.html.

———. 2013b. "National Money Laundering and Terrorist Financing Risk Assessment." https://www.fatf-gafi.org/media/fatf/content/images/national_ml_tf_risk_assessment.pdf.

For, Organisation. 2013. *Bribery and Corruption Awareness Handbook for Tax Examiners and Tax Auditors.* Paris: Organisation for Economic Cooperation and Development, Cop.

———. 2016. *Corruption in the Extractive Value Chain: Typology of Risks, Mitigation Measures and Incentives.* Paris: OECD Publishing.

———. 2021. *Fighting Tax Crime: The Ten Global Principles, Second Edition.* Paris: OECD Publishing.

Gamlen, Alan, Christopher Kutarna, and Ashby H. B. Monk. 2015. "Re-Thinking Immigrant Investment Funds." *SSRN Electronic Journal* 1 (1). https://doi.org/10.2139/ssrn.2689105.

Gardner, Howard. 1999. *Intelligence Reframed: Multiple Intelligences for the 21st Century.* New York: Basicbooks; Plymouth.

George Anthony Kulz. 2020. *Artificial Intelligence in the Real World.* Lake Elmo, Mn: Focus Readers.

Gregory, Sam. 2021. "Authoritarian Regimes Could Exploit Cries of 'Deepfake.'" Wired. 2021. https://www.wired.com/story/opinion-authoritarian-regimes-could-exploit-cries-of-deepfake.

Grenada Citizenship by Investment Act. 2013.

H20.ai. 2017. "Using Artificial Intelligence and Machine Learning to Help Financial Institutions Increase Compliance with Know Your Customer (KYC) Regulations Solution Brief." https://www.h2o.ai/wp-content/uploads/2017/06/Know-Your-Customer_v3_pages.pdf.

Haugeland, John. 2000. *Artificial Intelligence the Very Idea.* Cambridge, Mass. [U.A.] MIT Press.

Kurzweil, Ray. 1999. *The Age of Intelligent Machines.* Cambridge, Mass.: MIT Press.

Malhotra, Diksha, Poonam Saini, and Awadhesh Kumar Singh. 2021. "How Blockchain Can Automate KYC: Systematic Review." *Wireless Personal Communications*, August. https://doi.org/10.1007/s11277-021-08977-0.

Maltese Citizenship Act. 2014. Vol. 188.

Mcgee, Robert W. 2012. *The Ethics of Tax Evasion: Perspectives in Theory and Practice.* New York: Springer.

Mitrou, Lilian. 2018. "Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?" *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3386914.

Morehead, Hugh. 2018. "A Beginners' Guide to Investment Migration." The Review Magazine. Life. Style. April 14, 2018. https://www.thereviewmag.co.uk/a-beginners-guide-to-investment-migration/.

Mozur, Paul, and John Markoff. 2017. "Is China Outsmarting America in A.I.?" *The New York Times*, May 27, 2017, sec. Technology. https://nyti.ms/2r8aHFZ.

Norvill, Robert, Cyril Cassanges, Wazen Shbair, Jean Hilger, Andrea Cullen, and Radu State. 2020. "A Security and Privacy Focused KYC Data Sharing Platform." *Proceedings of the 2nd ACM International*

Symposium on Blockchain and Secure Critical Infrastructure, October. https://doi.org/10.1145/3384943.3409431.

OECD. 2018. "OECD DUE DILIGENCE GUIDANCE for RESPONSIBLE BUSINESS CONDUCT." http://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf.

———. 2019a. *Artificial Intelligence in Society.* Paris Organisation for Economic Co-Operation and Development - OECD.

———. 2019b. *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors.* Paris - OECD.

Organisation for Economic Co-Operation and Development. 2008. *Study into the Role of Tax Intermediaries.* Paris: OECD.

Oxford Analytical. 2020. "Due Diligence in Investment Migration." https://www.refinitiv.com/content/dam/marketing/en_us/documents/partners/due-diligence-in-investment-migration-best-approach-and-minimum-standard-recommendations.pdf.

Poole, David L, Alan K Mackworth, and Randy Goebel. 1998. *Computational Intelligence: A Logical Approach.* New York: Oxford University Press.

Ranchordas, Sofia. 2021. "Experimental Regulations for AI: Sandboxes for Morals and Mores." *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3839744.

Russel, Stuart, and Peter Norvig. 2018. *ARTIFICIAL INTELLIGENCE: A Modern Approach.* Prentice Hall.

Smuha, Nathalie A. 2019. "The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence." *Computer Law Review International* 20 (4): 97–106. https://doi.org/10.9785/cri-2019-200402.

St. Kitts and Nevis Citizenship by Investment Regulations. 2011.

St. Lucia Citizenship by Investment Act. 2015.

Sunstein, Cass R. 2021. "Governing by Algorithm? No Noise and (Potentially) Less Bias." *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3925240.

Svan den Berg. 2021. "Dutch Government Quits over 'Colossal Stain' of Tax Subsidy Scandal." Reuters.

Taylor, Bex. 2021. "Book Review: Invisible Women by Caroline Criado-Perez." *He Rourou* 1 (1): 96–98. https://doi.org/10.54474/herourou.1.1.2920220.

The Wolfberg Group. 2019. "Wolfsberg Guidance on Sanctions Screening." https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf.

Verhage, Antoinette. 2011. *The Anti Money Laundering Complex and the Compliance Industry*. London: Routledge.