Open Access Library Journal
2024, Volume 11, e11453
ISSN Online: 2333-9721
ISSN Print: 2333-9705

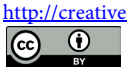
The Congolese Legislation Readiness against AI Development and Foreign Attacks and Perspective of International Cooperation

Jordy Cloud Ntsoumou Mboulou

Faculty of Law, Beijing Normal University, Beijing, China
Email: cloudjordy97@gmail.com

How to cite this paper: Mboulou, J.C.N. (2024) The Congolese Legislation Readiness against AI Development and Foreign Attacks and Perspective of International Cooperation. *Open Access Library Journal*, **11**: e11453.
https://doi.org/10.4236/oalib.1111453

Received: March 18, 2024
Accepted: May 28, 2024
Published: May 31, 2024



Abstract

Artificial Intelligence (AI) has become an increasing concern for national cybersecurity in most countries, the Republic is no exception. The Republic of Congo is among the growing number of African countries to enact various legislation on cyber security and is also part of the African Convention on Cybersecurity and Personal Data Protection. Therefore, the country has three major laws: the Personal Data Protection Law, the Cybersecurity, and the law Cybercrime Law. These three laws although sufficient to tackle the most basic aspect of cybersecurity, do not provide room for AI, leaving a void in its use, integration in cybersecurity protection and protection against foreign body attacks especially those using AI as a tool or target. The ideal course of action will be for the Congo to take immediate action to solve this issue. While solving this issue, the country can rely on an extensive interpretation of its current laws to secure national cyberspace. The development of international norms on AI will be a great help in the fact that it will boost national cybersecurity by deterring the rise of dangerous AI use.

Subject Areas

Law

Keywords

Artificial Intelligence (AI), Congo, Congolese Legislation, Cyber Threat, Foreign Attack, International Cooperation, AI Military Application

1. Introduction

Artificial Intelligence (AI) is a vintage technology that dates to the father of computing Alan Turing [1] who theorized machine learning. Established as an

academic discipline in 1956 [2], AI evolved in two directions. The first focuses on cognitive capabilities trying to replicate the brain's ability to process symbols. and the second on neuronal networks to create an inclusive and connective approach in machine learning [1]. The advent of big data has favored the development of more sophisticated AI systems aiming at studying and classifying data for better faster processes leading to the democratization of AI in the computing industry. AI quickly became the technology of the future.

Throughout its lifetime, AI is intricate to data, the latter has become subject to increasing unlawful attacks using the most advanced technologies: AI. In response, states are improving their legislation to secure data and promote good use of AI. Hence our concern for the Republic of Congo, the country in a central part of Africa, with a growing interest in technology and data security in face attacks.

The imperative to regulate AI is widely acknowledged, yet the Congo lags behind in this regard, with no indication of forthcoming legislation. This paper ought to answer the question: Is Congolese legislation equipped to face the AI wave and threats related? Furthermore, the proliferation of AI and its potential risks, including cyber terrorism and warfare, necessitates international cooperation to establish protection standards and facilitate knowledge exchange between advanced and developing nations. AI's transformative capabilities pose both opportunities and challenges and addressing global inequalities in AI readiness is crucial for preserving peace and protecting human rights. Thus another key interrogation: can international cooperation be the way to establish adequate protection for small countries like Congo?

The present work studies AI legislation in the Republic of Congo in order to assert the level of protection against foreign attacks. We will reflect on necessary legislative changes in order to better use AI in the protection of Congolese cyberspace. Furthermore, an analysis of data protection structures and legislation will be done. Finally, we will envision the possible international measures to be taken to manage AI and its threat to cybersecurity globally.

In this study, we will (I) have a literature review on the subject (II) Understand the notions of AI and foreign attack, then present (III) the Congolese legislation (IV) and its possible improvements. The final part will analyze (V) international cooperation on AI.

2. Literature Review

Since its inception, artificial intelligence (AI) has garnered significant scholarly attention, predominantly within the realm of information technology (IT) and related sciences. However, over the past decade, research has expanded into other fields such as humanities and law, reflecting the increasing influence of AI on society. Despite earlier focus on the necessity and feasibility of AI regulation, progress in this area has been limited, with countries like China and the US showing reluctance to enact comprehensive regulations due to concerns about

impeding innovation. Nonetheless, China has established standards for AI technology. Current researches focus less on the necessity of AI regulation legislation but rather on the most efficient regulation [3] [4], although most research focus on national legislation some are tackle the eventuality of regulation convergence or international harmonization. Regarding international cooperation on AI regulation important concerns are raised such as the minimum level of protection, the prime beneficiaries of the standard and the risk to failure [3] which causes a lot of skepticism about the feasibility of such an approach.

Furthermore, AI's dual application in civilian and military contexts underscores its complex nature. While civilian applications have been extensively studied through a legal lens, military applications have received less attention, remaining largely within the domain of hard sciences like physics and IT. This highlights the sensitivity surrounding AI's military use and the need for careful consideration. Although most AI developments are civilian-oriented, the potential misuse or deliberate targeting of AI, even in civilian contexts, can pose significant threats. In regions like the Congo, where research on AI is lacking and legislation is nonexistent, the urgency to address these issues is evident.

3. Understand AI and the Foreign Attacks

Understanding AI both as a concept, technology, its development, and its use is essential to the development of appropriate legislation. On the other hand, foreign attacks can vary depending on the jurisdiction.

3.1. Definitions of Artificial Intelligence

In its most basic form, "*Artificial intelligence* (*AI*) *is the intelligence of machines or software*, *as opposed to the intelligence of human beings or animals*" [2]. It is "*the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings*" [5]. In its current form, AI is used for advanced web search engines, recommendation systems, understanding human speech, self-driving cars, generative or creative tools, and also in the gaming industry.

The normative definition that inspires most legislation is found in the Recommendations of OECD's Council on Artificial Intelligence: "an *AI system is machine-based system that can*, *for a given set of human-defined objectives*, *make predictions*, *recommendations*, *or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy*" [6]. This definition has an echo in the EU's [7] and Chinese[8] AI regulation. We can summarize AI as "a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives" [9].

3.2. Foreign Attacks

Foreign bodies' attacks are unlawful attempts by national or nonnational hackers

or structures from or located on another territorial jurisdiction to disrupt national cybersecurity. Their aim at access directly or indirectly, size or corrupt all of part of the cybersecurity structure of a country. These threats are diverse, we will focus on those using AI or targeting AI-powered systems.

1) Threats on security

Are the threats related to state security or defense installation [10]. These are attacks on defensive structures mostly powered by AI or machine learning algorithms. Hackers use AI to scan and detect breaches or soft links in security structures and establish a pattern of attack aimed at that specific aspect in order to disrupt, destroy security systems or extract, suppress or corrupt critical data.

Much dangerous, are attacks on weaponry systems that drive a lot of concern and pushbacks even by state officials [11]. The weaponry application of AI involves the creation of "*Autonomous weapon*", weapons that can be man-assisted or completely automatized. In the current state of affairs, the is no official non-man-assisted weapon. However, there are ongoing breakthroughs that could lead to their creation. Once in use, these weapons should be able to detect physical attacks and retaliate with sufficient power to deter or annihilate original threats. With this type of weapon, any cyberattack can ignite a world war flame.

2) Threats on Data

There are various types of data-related threats, and they all aim at accessing, using, or transferring protected data. The data-related threats target mostly data-collecting vectors such as:

In social media [12], AI attacks target social media because the enormous amount of data provided. It can also be used to spread inductive contact or fake news for the purpose of direct attacks.

Computing device [13]: whether it is personal computers or a high computing device, both contain data that attract foreign intelligence or other cyber criminals. Using AI hackers scan through the various layers of protection to extract data or introduce malware that can serve to disrupt the functioning of said devices.

Internet of Things (*IoT*) *devices* [13]: Are spread devices that become more and more part of our daily life. However, they can provide a backdoor for hackers to access a particular network or communication system and proceed with its attack.

4. The Congolese Legal Landscape

We will be examining the Congolese legislative terrain related to AI, giving an overview of pertinent laws and an analysis of their limitations when confronted with the evolving challenges faced.

Applicable Laws and Regulations

The Congolese nation's legal arsenal in regard to cybersecurity is composed of:

1) ***African Convention on Cybersecurity*** [14]: essentially a soft law designed to urge and help member state in establishing their own cybersecurity laws and

regulations. It provides different requirements for each aspect of cyber security such as Data protection, critical information infrastructure, cyber security agency, etc.

2) ***National cyber security law*** [15]:

It establishes the legal framework for the security of information system and electronic communication networks. More specifically it:

- organizes and coordinates the security of information systems and electronic communications networks.
- build the confidence of citizens, businesses and public authorities in information systems and electronic communications networks.
- laid down general rules for the protection of information systems and electronic communications networks.
- define the rules applicable to cryptographic means, modalities and systems and punish related offences. (article 1)

Cyber Security law is the foundation of digital legislation, it is the legislative equivalent of national cyber policies, it establishes the national cyber identity, distinguishes key aspects of state digital sovereignty, and allows subsequent legislation to emerge.

3) ***Data protection Law*** [16]:

Data protection law:

- sets up a system to ensure the protection of the fundamental rights and freedoms of natural persons, including their private lives, with regard to the processing of personal data.
- ensure that information and communication technologies remain at the service of the citizen and do not violate individual or public freedoms, in particular, privacy (article 1).

It is an important tool to ensure a proper use of personal data and constitutes a first step towards ethical norms thanks to its strict disposition on personal data use. Knowing that AI development and use imply large quantities of data as well as the impact on data subject, the data protection law is an important tool to help regulate AI.

4) ***Cybercrime Law*** [17]

The purpose of this law is to define and punish offenses related to Information and communication technologies. The provisions of the law apply to all persons, regardless of their nationality, who have committed an offense through information and communication technologies in the Republic of Congo (article 2), one can argue that it may also be applied against those whose actions constitute crimes against the Congolese states and or entities under its jurisdiction which is exactly the consequences of foreign attacks. The law provides various dispositions on crimes impacting national security or interests (articles 75-77) such as processing (including accessing, deleting or destroying) important state data and/or providing them to foreign entities. Under these stipulations, actions meant to directly or indirectly giving foreign entities access to certain type of information or data should be prosecuted, through the use of digital tools like AI it

is difficult to track down or establish a direct author of the crime, in the eventuality of such successful track, it will still be difficult to prosecute the author due the protection offers to them by their state. These dispositions are more efficient when at least one of the entities or personnel is physically on the Congolese territory otherwise, only pollical maneuver can help solve these issues.

5. Weaknesses and Insufficiencies

The Congolese legal system as multiple weaknesses, we will focus on the most notable.

1) Data Protection Authority (DPA)

Law No. 29-2019 provides for specific procedures for the fulfilment by data controllers of their data processing obligations (*articles 31-45*). It applies to any processing, automated or not, carried out on the territory of the Republic of Congo or in any place where the law of that country applies (*article 2*). It is also applicable to any processing carried out by a controller established in the Congo or outside the Congo but whose means of processing are located on Congolese territory (*article 2*). Regrettably, its enforcement is greatly hindered due to the absence of Data Protection agency. Article 4 Paragraph 2 of the said Law provides for the creation of a Data Protection Agency referred to as "*the Commission*", responsible for the Protection of personal data and ensuring compliance with data protection law. However, the law does not contain detailed provisions on its composition, organization, member appointment, independence, and budget. Consequently, by the time of the present redaction, the said commission has not been officially created or its commissioners appointed.

A special case can be made for defense and security organs. The Military is isolated from all the systems (*article 3 Cybersecurity Law*), at the same time, no laws has been enacted to organize security and defense data protection. Everything related to that aspect is directly dealt with through internal rules and regulations making it impossible for outsiders to assert how secure are sensitive data in that area. The reason might be the risk of external attacks, indeed not disclosing their information on the subject can instill potential doubt on hackers who cannot know how to organize the protection system.

In the absence of a cybersecurity agency and DPA, the cybersecurity landscape of the Congo seems quite deserted. It is hard and even impossible to correctly prevent attacks on personal data or other cybersecurity aspects. It is also difficult to foresee malfunction and leaks in the overall nation's cyberspace.

2) Lack of Cybersecurity Regulatory Authority

Despite the provision of article 27:1 (a) of the convention [18], the Congo has not yet established an independent authority in charge of national cybersecurity. This makes it difficult to implement and enforce regulation in all domains of cybersecurity. Therefore, in practice, the Congo does not have a functioning cyber security system. However, the Congo established: the Congolese Information System Agency [19]. It is responsible for developing and implementing appropriate information systems plans, adapted to the specific needs of the State (ar-

ticle 3 Law 2/2015).

3) Absence of an AI-related law or regulation.

The Congolese cybersecurity legal landscape does not include any AI-related law. As seen with already existing laws, the country lacks proper enforcement. This is due to the fact that implementing cybersecurity laws and regulations requires a certain level of capability (both in terms of equipment and human resources) which also implies adequate funding. The meager budget and poor education level are important hindrances to a good cybersecurity structure. Thus, the country focuses on providing minimum coverage protecting first national defense structures by isolating them from the civil network and encouraging network providers and finance actors to improve their protection mechanisms.

The absence of law also hinders the integration of AI in the national cybersecurity defense mechanism, leaving cyberspace vulnerable to intrusion via new system deployment. The absence of proper AI legislation constitutes an even bigger threat considering that most citizens and entities already use various foreign-made AI tools without any control, this may constitute an open door for attacks. Similar to the requirement made by the data protection law in article 3, it might be important to consider having representatives of certain AI developers in order to establish control and help develop important rules and mechanisms to better protect citizens and entities including state organs.

6. Perspective on Legislation Improvement

The legislative void in the Congolese legal landscape should be filled by well-written and structured AI law. The best course of action would be to learn from others regulations.

6.1. Regulations around the World

AI regulation should include a clear definition panel, a purpose and rightful use of the technology, equipment standard, transparency and data usage aspect, responsibilities, and sanctions. We will have a look at two of the prominent legislations on the subject: the EU and the Chinese Regulations.

The definition and scope of application: it is the starting point of any legislation it helps establish clear boundaries that distinguish it from other technology and digital products [4]. It should also be flexible enough [5] to include future variant or any form of evolution of AI technology as does the EU AI Regulation [7]. In the Chinese Artificial Intelligence Development Plan [20], is given a list of applications and potential uses of AI that's help understand deeply the notion.

Use: a good regulation should outlaw the dangerous use of AI, those that have a negative impact on people's rights, well-being, social stability, economic order and overall security and national interest. In that regard, the Chinese have condensed them into six key aspects [21]. On the other hand, the EU has a set of prohibited uses [7].

Technology standard and classification: the legislation should classify dif-

ferent categories of AI in order to better regulate and safeguard rights, liberties, and interests. The EU regulation for example establishes a risk-based classification [7] [21].

Data management: AI heavily relies on data throughout every step of its existence, thus the necessity to establish safer and adequate data management and protection. It should cover both the conception and usage phases [7] [21].

Responsibility [22] [23]:

AI possesses serious responsibility; the legislator should establish clear responsibility and liability at every step of AI's lifetime. An emphasis should be put on distinguishing users' and operators' responsibility, specific procedures should be set for both.

6.2. The Suitable Legislative Choice for the Congo

The adoption of comprehensive legislation targeting AI, although helpful, is not yet envisioned in the near future. Furthermore, the high probability of enacting an empty law with any effective enforcement mechanism makes it less desirable. One can argue the necessity of having a law even in the absence of real enforcement as it constitutes a first step toward progress and can also deter some malicious attempts. However, in this case, it will increase the burden of an already exhausted state to establish structures and norms that will not be correctly applied if at all.

Jacob Turner [24] considers that legislation can be classified in three categories: promoting the growth of a local AI industry, ethics and regulation of AI and tackling the problem of unemployment caused by AI [25]. The Congo is an AI consumer thus, is less likely to develop the first category of legislation. Advanced economies are equipped to capture growth generated through AI development while The Congo still has a long way before reaching such a level. The same is true for the third category, considering the underdevelopment and poor regulation on the Congolese labor market, there is still no incentive to develop such regulation.

The adoption of ethical norms of AI seems to be a more reasonable approach providing fewer constraints while making up for the absence of regulation. Ethical norms provide the flexibility needed to develop technology while guaranteeing users' safety. It also provides a basis for AI integration into national cyberspace protection allowing actors to choose approved AI systems able to integrate national cybersecurity networks and detect threats.

These norms should provide guidance on transparency, Developer should comply with a level of transparency [4] over data used to train and control AI systems to reduce bias risk and discrimination risk especially imported, transparency should be a norm of control. Additionally, Mechanisms of complaints and liability should be set by the developers and the state to achieve a higher effective rate. Additionally, developers should bear the burden of proof considering the difficulty faced by users to understand, access the technology and provide adequate proof.

6.3. Alternative Measures in Absence of Legislation Upgrade

Considering the current situation, in the absence of any AI legislation, we can still find rules applicable to AI in many aspects, especially those that matter the most. For example, using article 4 of the cybercrime law, we can obtain legal basis for prosecuting anyone hacking activity using AI to fraudulently attempt or to access any information system. We can also use the dispositions of articles 6 of the cybercrime law disposition to punish cyberattacks aiming or resulting at disturbing, hindering, or even shutting down communication and information systems.

The current Congolese legal system is equipped enough to deal with many basic and recurrent aspects of AI threats, the emphasis should be put first on more enforcement in order to guarantee people's safety. Once proper enforcement of existing regulations is done further legislative endeavors can be engaged with the same achievement goal.

7. International Cooperation on AI

Global regulation or treaty in cybersecurity is a hard task to achieve considering the importance of the field and the diverging interests of each major actors[1]. Indeed, each state has its own reason and priorities when it comes to establishing AI policies and regulations. The current most important actors are the US, the EU, CHINA, in a less prominent spot, Japan [25] and Russia each of them with their own political agenda [11] as well as a regulatory approach [9]. Therefore, achieving a consensus on such a hot topic is a titanic task that government and political actors tend to avoid due to the turmoil that it can cause on a domestic level. Certain countries like the US expect their counterpart to make the first concession while not giving enough in return if nothing at all [26], which hinders others like CHINA and RUSSIA from furthering their goodwill. Not only do interests tend to vary on the most important topic, but sometimes are opposites for various reasons.

In the recent resolution A/78/L.49 the UN General Assembly [27] has highlighted the need to set international cooperation on AI to address issues on human rights, equality, protection, and access of developing countries as well as the overall progress towards a stable and peaceful world by limiting risks, threats, and military use of AI. This resolution echoes a first attempt to offer a globalized solution to problems faced by developing countries regarding AI development, it establishes implicitly international cooperation as an indispensable part of the solution. It is thus necessary to further effort and cooperation between states to tackle some global issues like AI weaponry, human right, and criminal use.

7.1. In Weaponry

The twentieth century has taught us the impact of massive weapon capabilities and our ability to limit arsenal expansion and prohibit use. This should make us

realize the dangerous potential of AI weaponry especially automatized weapons also incentivize governments to take a position [28] against such threats to our global future and stability. Thus, an UN lead treaty or a multilateral treaty led by the US, China and other Security Council members would slow down the potential arms race while discouraging other actors from entering the competition.

7.2. In Human Right

On a human rights aspect, the EU [7] and China [21] already set best practice standards that can inspire a worldwide treaty. The objective is to guarantee Transparency [29].

Transparency in data collection and use. Users should be able to know enough about the type or composition of the original data used to train AI and have a better understanding of his/her own generated data. The user should also be able to understand all or most of the implications and risks related to its use. Finally, the freedom to start and terminate a user agreement contract shall be followed by a right to dispose of generated data in the most effective way.

A security assessment could be envisioned but would imply multiple security standards and be detrimental to AI providers. Nonetheless, a right to timely inform about potential, imminent threats leaks or attacks should suffice.

7.3. In Cybercriminality

The definition and classification of criminal acts and their accountability pose a serious problem[1]. We should enhance security cooperation in regard to important domains like banking and market systems in order to protect, track and punish attacks on such indispensable sectors. Economic interconnection has made all countries interdependent on the global economic structure. It is our duty to protect such structures in cyberspace as well. A major concern can be cyber terrorism; indeed the spread of technology might provide additional ground and tools for terrorist groups or other criminal organizations to extend their criminal action. The recent increase in attacks and breaches [30] [31] shows how criminals are adapting to cyber security infrastructures of advanced countries. This implies that less developed countries are easier. When most criminals target advanced countries for the vast resources they possess, terrorists are moved by ideology and attack more frequently small countries against which they have important leverage. If transposed in cyberspace, a terrorist attack will not only aim at stilling data and information but also cripple targeted countries causing important loss. Thus the necessity to help small country such as Congo to achieve a certain level of protection to avoid catastrophe far beyond the scale of the WannaCry Attack [32]. Only international cooperation can lead to said results.

7.4. Bilateral and Multilateral Agreement

While waiting for a global move towards AI regulation, we can encourage bila-

[1]Andrés, M. B. (2021.). Towards legal regulation of Artificial Intelligence "Hacia la regulación jurídica de la inteligencia artificial". NUEVA ÉPOCA VOL. 15, No. 48: PP35-53.

teral and multilateral cooperation. This might be a longer and tedious but stabler, more efficient and sustainable process. It guarantees the full commitment of all parties to such initiatives and spreads best practices and values. The Treaty on Nonproliferation of Nuclear Weapons [33] or agreements under the WTO [34] are valuable proofs. Countries with the same concerns can easily reach an agreement. We know China's concerns for its cyberspace sovereignty and data territoriality, these concerns although present in the West have different components and focus. China focuses on assuring robust and uniform security control on data generated its legal subject, thus the importance of territorial storage of said data in order to monitor both physical and cybersecurity. On the other hand, the US focuses on a more liberal approach pushing for easier transnational flow of data while encouraging companies to increase their respective level of protection. However, the Chinese concerns have a better echo in Russia. Due to the recent development, the need for more cyber sovereignty has increased threats to its cybersecurity occasioned by the ongoing war. Furthermore, the economic rapprochement between Russia and China has set the ground for cooperation. It would be easier for both countries to agree on mutual terms regarding AI bilateral ethical norms, data protection against foreign body attacks and attempts or AI use in cyber criminality.

The reverse side of this approach is that it increases the risk of further antagonizing states with diverging interests by more or less homogenous groups that have similar or converging interests. Indeed, Countries prefer to be binding with countries whose ideology and core interests are similar. Although the US, Canada, EU countries, England, Australia, and New Zealand don't always have the same interests, they will tend to choose a common approach on the international scene when it comes to dealing with issues presenting a serious ideological and political component such as AI, this is reinforced by existing cooperation between most of these countries [35]. Consequently, any treaty on the subject will most likely create factions between countries aligning politically or historically with the WEST, those that diverge (like China or Russia) and those caught in the middle, like the Congo. In such eventuality, legal norms can flourish inside factions focusing on different aspects of AI governance while outside harmonization will be difficult. In such scenario global consensus would be even further out of reach than it is today. In fact, recent developments [36] lead to believe that such cooperation is now envisioned between both countries with an eventuality of including AI weaponry systems. When at fruition such cooperation will send a strong message to the international community, hopefully attracting other countries. However, an analysis of present tendencies suggests that antagonism between blocks and countries will increase. Indeed, the US and its allies distrust the actions of China and Russia thus sparking an opposite measure to contain what their perceive as a threat [37] instead of seeing the opportunity to engage in serious talk on the subject to avoid future escalation.

On a second consideration, even such a situation can promote relative stability and harmonization in AI best practice by business and other economic actors

active on the international field. Due to their activities, AI developers offering service under multiple jurisdictions will have to integrate different compliance requirements in their product leading to a product that can easily be commercialized under any jurisdiction.

Hopefully, the future and geopolitics are incredibly unpredictable which gives us more confidence in hoping for a better outcome by successive and mutual cooperation.

8. Conclusion

AI development is attracting more state attention, pushing for legislative action to guarantee cybersecurity and data protection. The Republic of Congo although lacking specialized legislation is equipped with a broad and flexible set of laws that can provide a certain level of protection against foreign bodies' threats. Nonetheless, there is room for growth in order to establish Congolese legislation hopefully authorities will enact the appropriate laws. On the international stage, we are far from achieving any legislative breakthrough, some observations ignite the flame of possibilities.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Copeland, B.J. (2023) Artificial Intelligence. Encyclopedia Britannica. https://www.britannica.com/technology/artificial-intelligence

[2] Wikipedia (2023) Artificial Intelligence. https://en.wikipedia.org/wiki/Artificial_intelligence

[3] De Almeida, P.G.R., Dos Santos, C.D. and Farias, J.S. (2021) Artificial Intelligence Regulation: A Framework for Governance. *Ethics and Information Technology*, **23**, 505-525. https://doi.org/10.1007/s10676-021-09593-z

[4] Buiten, M.C. (2019) Towards Intelligent Regulation of Artificial. *European Journal of Risk Regulation*, **10**, 41-59. https://doi.org/10.1017/err.2019.8

[5] Smuha, N.A. (2021) From a 'Race to Ai' to a 'Race to Ai Regulation': Regulatory Competition for Artificial Intelligence. *Law, Innovation & Technology*, **13**, 57-84. https://doi.org/10.1080/17579961.2021.1898300

[6] OECD (2019) Recommendation of the Council on Artificial Intelligence. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[7] European Union (2023) Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.

[8] MIIT (2018) Artificial Intelligence Standardization White Paper. Ministry of Industry and Information Technology, Beijing.

[9] Schildkraut, P. and Zhang, H. (2023) What to Know about China's New AI Regulations. Law360.

[10] Khalifa, E. (2021) Artificial Intelligence and Global Security. https://www.researchgate.net/profile/Ehab-Khalifa/publication/356207786_Artificial_Intelligence_and_Global_Security/links/6192244cd7d1af224bef7bbe/Artificial-Int

elli-
gence-and-Global-Security.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

[11] Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V. and Floridi, L. (2020) The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation. *AI & Society*, **36**, 59-77. https://doi.org/10.1007/s00146-020-00992-2

[12] Granados, A. (2023) The Privacy Paradox of AI: Emerging Challenges on Personal Data.
https://velaro.com/blog/the-privacy-paradox-of-ai-emerging-challenges-on-personal-data#:~:text=The%20unchecked%20use%20of%20AI%20technologies%20could%20lead,intentional%20or%20unintentional%20bias%20and%20lack%20of%20transparency

[13] Saxena, R. and Gayathri, E. (2022) Cyber Threat Intelligence Challenges: Leveraging Blockchain Intelligence with Possible Solution. *Materials Today*: *Proceedings*, **51**, 682-689. https://doi.org/10.1016/j.matpr.2021.06.204

[14] Congo (2020) Law No. 43-2020 African Union Convention on Cybersecurity and the Protection of Personal Data Ratification Law 08/20/2020. Republic of Congo: National Official Journal, Brazzaville.

[15] Congo (2020) Law No. 26-2020 on Cybersecurity 05/06/2020. Republic of Congo: National Official Journal, Brazzaville.

[16] Congo (2019) Law No. 29-2019 on Personal Data Protection. Republic of Congo: National Official Journal, Brazzaville.

[17] Congo (2020) Law No. 27-2020 on Combatting Cybercrime. Republic of Congo: National Official Journal, Brazzaville.

[18] AU (2014) African Union Convention on Cyber Security and Personal Data Protection. Assembly of the Union, Malabo.

[19] Congo (2015) Law No. 2-2015. Republic of Congo: National Official Journal, Brazzaville.

[20] People's Republic of China (PRC) (2017) New Generation Artificial Intellegence Development Plan (GAIDP). State Council, Beijing.

[21] The National New Generation Artificial Intelligence Governance Specialist Committee (2021) Ethical Norms for New Generation Artificial Intelligence Released.
https://cset.georgetown.edu/wp-content/uploads/t0400_AI_ethical_norms_EN.pdf

[22] EU (2023) Explanatory Memorandum on the Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial.
https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

[23] CAC (2023) Measures for the Management of Generated Artificial Intelligence Services, National Internet Information Office.
https://www.pwccn.com/en/industries/telecommunications-media-and-technology/publications/interim-measures-for-generative-ai-services-implemented-aug2023.html

[24] Jacob, T. (2018) Robot Rules. Palgrave Macmillan, Cham.
https://doi.org/10.1007/978-3-319-96235-1

[25] Andrés, M.B. (2021) Towards Legal Regulation of Artificial Intelligence "Hacia la regulación jurídica de la inteligencia artificial". *Revista IUS*, **15**, 35-53.

[26] Goldsmith, J. (2011) Cybersecurity Treaties: A Skeptical View. In: Berkowitz, P., Ed., Future Challenges in National Security and Law, Hoover Institution, Stanford.

https://www.hoover.org/sites/default/files/research/docs/futurechallenges_goldsmith.pdf

[27] United Nations (2024) Landmark Resolution on the Promotion of "Safe, Secure and Trustworthy" Artificial Intelligence (AI) Systems that Will also Benefit Sustainable Development for All. https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf?token=tuc2PzWtoM7xVcPEUE&fe=true

[28] PRC Delegation (2023) The Position Paper Submitted by the Chinese Delegation to CCW 5th Review Conference. https://www.unog.ch/80256EDD006B8954/(httpAssets)/DD1551E60648CEBBC125808A005954FA/$fle/China's+Position+Paper.pdf

[29] Kerry, C.F. (2020) Protecting Privacy in an AI-Driven World. https://www.brookings.edu/articles/protecting-privacy-in-an-ai-driven-world/

[30] Walsh, N.P. (2021) Serious Cyberattacks in Europe Doubled in the Past Year, New Figures Reveal, as Criminals Exploited the Pandemic. https://www.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html

[31] Kosling, K. (2024) Data Breaches and Cyber Attacks in Europe in January 2024-2,111,560,354 Records Breached. https://www.itgovernance.eu/blog/en/data-breaches-and-cyber-attacks-in-europe-in-january-2024-2111560354-records-breached

[32] National Audit Office (2017) Investigation: WannaCry Cyber Attack and the NHS. https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/#downloads

[33] UN (2015) The 2015 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT). New York. https://undocs.org/NPT/CONF.2015/50(PartIII)

[34] Hoffmana, S.J., Baral, P., Van Katwyk, S.R., *et al.* (2022) International Treaties Have Mostly Failed to Produce Their. *Proceedings of the National Academy of Sciences*, **119**, e2122854119.

[35] France Embassy in London (2021) Digital diplomacy—Launch of the Global Partnership on Artificial Intelligence by 15 Founding Members—Communiqué Issued by the Office of the Minister of State for the Digital Sector. https://uk.ambafrance.org/France-among-15-nations-creating-Global-Partnership-on-AI

[36] Paleja, A. (2024) Russia and China Ditch US Proposal, Swap Notes on the Military Use of AI. https://interestingengineering.com/military/russia-china-team-military-use-of-ai

[37] Bendett, S. and Kania, E.B. (2019) A New Sino-Russian High-Tech Partnership. https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2019-10/A%20new%20Sino-Russian%20high-tech%20partnership_0.pdf?VersionId=xAs9Tv5F.GwoKPiV9QpQ4H8uCOet6Lvh