2024. I. évfolyam 4. szám

STUDIA IURIS

Jogtudományi Tanulmányok / Journal of Legal Studies

KÁROLI GÁSPÁR REFORMÁTUS EGYETEM

ÁLLAM- ÉS JOGTUDOMÁNYI DOKTORI ISKOLA

STUDIA IURIS

Jogtudományi Tanulmányok / Journal of Legal Studies

2024. I. évfolyam 4. szám

Károli Gáspár Református Egyetem
Állam- és Jogtudományi Doktori Iskola

A folyóirat a Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskolájának a közleménye. A szerkesztőség célja, hogy fiatal kutatók számára színvonalas tanulmányaik megjelentetése céljából méltó fórumot biztosítson.
A folyóirat közlésre befogad tanulmányokat hazai és külföldi szerzőktől – magyar, angol és német nyelven. A tudományos tanulmányok mellett kritikus, önálló véleményeket is tartalmazó könyvismertetések és beszámolók is helyet kapnak a lapban.
A beérkezett tanulmányokat két bíráló lektorálja szakmailag. Az idegen nyelvű tanulmányokat anyanyelvi lektor is javítja, nyelvtani és stilisztikai szempontból.
A folyóirat online verziója szabadon letölthető (open access).

Kiadó: Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskola
Székhely: 1042 Budapest, Viola utca 2-4
Felelős Kiadó: Tóth J. Zoltán

A tipográfia és a nyomdai előkészítés Csernák Krisztina (L'Harmattan) munkája
A nyomdai munkákat a Robinco Kft. végezte, felelős vezető Gembela Zsolt

Honlap: https://ajk.kre.hu/index.php/jdi-kezdolap.html
E-mail: doktori.ajk@kre.hu
ISSN 3057-9058 (Print)
ISSN 3057-9392 (Online)
URL: KRE ÁJK - Studia Iuris
https://ajk.kre.hu/index.php/kiadvanyok/studia-iuris.html

TARTALOMJEGYZÉK

HOW CLIMATE CHANGE AFFECTS PUBLIC INTERNATIONAL LAW

Muhanad Alamro[1]

ABSZTRAKT ■ Ez a tanulmány a klímaváltozás és a nemzetközi jog metszetét vizsgálja, különös tekintettel az emberi jogokra és a tengerjogi szabályozásra. Az emberi jogok összefüggésében megvizsgálja a klímaváltozás hatásait az élethez és az önrendelkezéshez való jogokra, valamint a tiszta környezethez való hozzáférésre vonatkozóan, kiemelve az egyre változó jogi környezetet és a nemzetközi emberi jogi mechanizmusokban történt legutóbbi fejleményeket. Ezen túlmenően mélyebben foglalkozik a klímaváltozás tengerjogi szempontjainak következményeivel, elemezve az UNCLOS kötelezettségeket, a nemzetközi törvényszékek szerepét, valamint a jogi keretrendszerek alkalmazhatóságát a klímaváltozással kapcsolatos kihívások kezelésében a tengeri kormányzás területén. Átfogó szakirodalmi áttekintés és esettanulmányok elemzése révén ez a tanulmány rávilágít a klímaváltozás komplexitásaira a nemzetközi jog területén, és hangsúlyozza a kollektív cselekvés fontosságát annak káros hatásainak enyhítése érdekében.

ABSTRACT ■ This study examines the intersection of climate change and international law, with a focus on human rights and the Law of the Sea. In the context of human rights, it explores the impacts of climate change on the rights to life, self-determination, and access to a clean environment, highlighting the evolving legal landscape and recent advancements in international human rights mechanisms. Furthermore, it delves into the implications of climate change for the Law of the Sea, analyzing UNCLOS obligations, the role of international tribunals, and the applicability of legal frameworks in addressing climate-related challenges in maritime governance. Through a comprehensive review of relevant literature and case studies, this study sheds light on the complexities of climate change within the realm of international law and underscores the importance of collective action to mitigate its adverse effects.

Kulcsszavak: klímaváltozás, emberi jogok, nemzetközi jog, nemzetközi környezetjog, tengeri nemzetközi jog, nemzetközi törvényszékek

[1] PhD student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

1. Introduction

Climate change and international law are intricately linked, as the detrimental consequences of climate change threaten the enjoyment of various human rights globally. International law plays a crucial role in addressing climate change through treaties, agreements, and conventions aimed at mitigating greenhouse gas emissions, adapting to climate impacts, and promoting sustainable development.

The escalating adverse effects of climate change have prompted a scholarly inquiry into the capacity of international human rights mechanisms to afford adequate protection to those rights imperiled by climate change. Thus, international tribunals have highlighted on a strong connection between the obligations of States under international environmental law and the rights potentially affected by climate change[2].

As climate change continues to affect the planet, it has significant implications for the oceans and the legal frameworks governing them. Rising sea levels, ocean acidification, and changes in marine biodiversity are just some of the consequences of climate change impacting the seas. Therefore, as climate change increasingly affects the marine environment, the international law of the sea becomes ever more relevant in promoting sustainable ocean governance and addressing the challenges posed by climate change.

2. Climate change and international human rights law

The United Nations Framework Convention on Climate Change (UNFCCC) defines "climate change" to mean a change of climate which is attributed directly or indirectly to human activity that alters the composition of the global atmosphere and which is in addition to natural climate variability observed over comparable time periods.[3]

[2] See, European Court of Human Rights (ECtHR) Judgment in the (Cordella case), it held that Italy had failed to fulfil its obligations under Directive 2008/1 EC of the European Parliament and of the Council concerning integrated pollution prevention and control. In the context of an infringement procedure against Italy, opened on 16 October 2014, the European Commission issued a reasoned opinion asking the Italian authorities to remedy the serious pollution problems observed. It noted that Italy had failed to fulfil its obligations to guarantee that the steelworks complied with the Industrial Emissions Directive ECtHR, Cordella and Others v Italy, App no 54514/13 and 54264/15 (ECtHR, 24 January 2019).

[3] UN General Assembly, United Nations Framework Convention on Climate Change: resolution / adopted by the General Assembly, 20 January 1994, A/RES/48/189.

This study aims to systematically examine the specific human rights most significantly affected by climate change, including but not limited to the right to life, the right to self-determination, and the right to access a clean, healthy, and sustainable environment.

2.1. Right to life

The right to life is considered as the most importantly basic right which has been affirmed by nearly all major human rights instruments. According to the article 3 of Universal Declaration of Human Rights *"everyone has the right to life, liberty and security of person"*, and also article 6 of the International Covenant on Civil and Political Rights states that: *"every human being has the inherent right to life"*.[4]

Although all States are committed to fulfil the right to life, Climate change clearly poses a threat to human life.[5] A recent report by the World Bank affirms this risk, finding that *" further health impacts of climate change could include injuries and deaths due to extreme weather events"*.[6]

The UN Human Rights Council (UNHRC) in 2008 expressed its concern that climate change is a direct and long-term threat to individuals and communities, with consequences for the full enjoyment of human rights.[7]

It is unequivocal that extreme weather events may be the most visible and most threat to the enjoyment of the right to life but they are by no means the only one. Climate change kills through drought, increased heat, expanding disease vectors and a myriad of other ways.

Notably, the International Court of Justice (ICJ) has revealed in Gabčíkovo Nagymaros case, that *"the environment is not an abstraction but represents the living space, the quality of life and the very health of human beings, including generations unborn"*.[8]

4 The United Nations Human Rights Committee describes the protection of life as a prerequisite for the enjoyment of all other human rights. See: Human Rights Committee :General Comment No. 36 (2018) on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life, UN Doc CCPR/C/GC/36 (30 October 2018) (General Comment No. 36) para 3.

5 Submission of the Office of the High Commissioner for Human Rights to the 21st Conference of the parties to the United Nations Framework Convention on Climate Change, 27 November 2015.

6 The World Bank:International Bank for Reconstruction and Development, turn down the heat: why a 4°C warmer world must be avoided, a report for the World Bank by the Potsdam Institute for Climate Impact Research and Climate Analytics, November 2012.

7 UNHRC Res (28 March 2008) UN Doc A/HRC/7/23.

8 Reports of judgments, advisory opinions and orders case concerning the Gabčíkovo Nagymaris project (Hungary Slovakia) judgment of 25 September 1997.

The European Court of Human Rights, through its interpretation of Article 2 on the right to life and Article 8 on private and family life, have recognized that States should hold positive obligations to prevent environmental risks that may endanger the right to life[9]. It affirmed in the Budayeva and Others v Russia case that in the context of dangerous activities the scope of the positive obligations under Article 2 of the Convention (right to life) largely overlaps with those under Article 8 (right to private, family life). Consequently, the principles developed in the Court's case-law relating to planning and environmental matters affecting private life and home may also be relied on for the protection of the right to life.[10]

The inter-American Court of Human Rights in its advisory opinion on the environment and human rights stated that the American Convention on Human Rights demands from parties to comply with the obligations to respect and ensure the rights to life and personal integrity, in the context of environmental protection, therefore the court will examine the procedural obligations relating to environmental protection in order to establish and determine the State obligations to respect and to ensure the rights to life established in the American Convention.[11]

Significantly, numerous national courts become more encouraged to protect the right to life in context to detrimental consequences of climate change, for example: on 20 December 2019 the Dutch highest court upheld the previous decisions in the 'Urgenda Climate Case,' a lawsuit originally brought by a Dutch environmental group Urgenda, on behalf of 886 citizens, against the Government. The court affirmed the lower courts' order requiring the Dutch Government to reduce greenhouse gas (GHG) emissions by a minimum of 25% by 2020 compared to 1990 levels, a target more ambitious than the one the Dutch State has under EU law (a 20% reduction by 2020 compared to 1990 levels). The court based its judgment on the UNFCCC and on the Dutch State's legal duties to protect the life and well-being of citizens in the Netherlands, in line with the European Convention on Human Rights (ECHR).[12]

[9] See, Öneryıldız v Turkey, App no. 48939/99 (ECtHR, 30 November 2004); Powell & Rayner v UK, App no 9310/81 (ECtHR, 21 February 1990); Hatton and Others v UK, App no 36022/97 (ECtHR, 8 July 2003); López Ostra v Spain, App no 16798/90 (ECtHR, 9 December 1994).

[10] Budayeva and Others v Russia, App no. 15339/02, 11673/02, 15343/02, 20058/02 and 21166/02 (ECtHR, 20 March 2008).

[11] Inter-American Court of Human Rights advisory opinion OC-23/17 of November 15, 2017 Requested by the Republic of Colombia, The Environment and Human Rights (State Obligations in Relation to the Environment in the Context of the Protection and Guarantee of the Rights to Life and to Personal Integrity: Interpretation and Scope of Articles 4(1) and 5(1) in Relation to Articles 1(1) and 2 of the American Convention on Human Rights).

[12] For more see: Benoit Mayer: The Contribution of Urgenda to the Mitigation of Climate Change. *Journal of Environmental Law*, 2/2023, 167–184.

2.2. Right to self-determination

In contrast to most human rights which are framed in individualistic terms, such as the right to life, self-determination is a collective right that enables groups to determine their political destiny and freely pursue their cultural, social, and economic development. The right to self-determination is well-defined in article 1 of the International Covenant on Civil and Political Rights (ICCPR)[13].

Climate change undeniably is posing an immediate and continued threat for low-lying Oceanic states. Without adaptation, the most vulnerable islands are anticipated to be uninhabitable by mid-century.[14]

According to a recent report by a group of United Nations Special Rapporteurs, climate change impedes the ability of peoples in small island states to live their traditional territory continuously, and threatens their right to self-determination[15]. Therefore, there is an argument to consider the capacity of the right of self-determination to levy a duty on large emitting States to reduce their greenhouse gas emissions, thereby reducing the risks of climate-change-induced displacement for vulnerable peoples.[16]

The prospect of total flooding of a small island State also threatens the right to self-determination. In the case of the land being flooded, there is a significant risk of a new form 'climate statelessness'[17]. Thus, those peoples might suffer deprivation of nationality without replacement by another nationality, they could have serious consequences in terms of preserving civil, political and

[13] The article 1 of ICCPR states:
"1. All peoples have the right of self-determination. By virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development.
2. All peoples may, for their own ends, freely dispose of their natural wealth and resources without prejudice to any obligations arising out of international economic co-operation, based upon the principle of mutual benefit, and international law. In no case may a people be deprived of its own means of subsistence.
3. The States Parties to the present Covenant, including those having responsibility for the administration of Non-Self-Governing and Trust Territories, shall promote the realization of the right of self-determination, and shall respect that right, in conformity with the provisions of the Charter of the United Nations."

[14] See, Curt D. Storlazzi et al.: Most Atolls Will Be Uninhabitable by the Mid21st Century Because of Sea-Level Rise Exacerbating Wave-Driven Flooding. *Science Advances*, 4/2018.

[15] Devandas Aguilar et al.: The effects of climate change on the full enjoyment of human rights (OHCHR, 2015), 16.

[16] Amy Maguire – Jeffrey McGee: A Universal Human Right to Shape Responses to a Global Problem? The Role of Self-Determination in Guiding the International Legal Response to Climate Change. *Review of European Community and International Environmental Law*, 1/2017, 61.

[17] See, Etienne Piguet: Climatic Statelessness: Risk Assessment and Policy Options. *Population and Development Review*, 4/2019, 865–883.

socio-economic rights such as, for example, the right of entry, residence, return and diplomatic protection.[18]

In May 2019 a communication was submitted to the United Nations Human Rights Committee by Torres Strait Islanders against Australia. The Islanders claimed that as Australia failed to adapt to climate change by, inter alia, upgrading seawalls on the islands and reducing greenhouse gas emissions, they have experienced direct harmful consequences on their livelihood, their culture and traditional way of life[19]. The U.N. Human Rights Committee found that Australia's failure to adequately protect indigenous Torres Islanders against adverse impacts of climate change violated their rights to enjoy their culture and be free from arbitrary interferences with their private life, family and home[20].

The Committee also has asserted in the Ioane Teitiota v. New Zealand case that without robust national and international efforts, the effects of climate change in receiving states may expose individuals to a violation of their rights under articles 6 or 7 of the International Covenant on Civil and Political Rights. Hence, the risk of an entire country becoming submerged under water is such an extreme risk that the conditions of life in such a country may become incompatible with the right to life with dignity before the risk is realized.[21]

2.3. Right of access to a clean, healthy, and sustainable environment

In July 2022 the UN General Assembly declared that everyone has a right to a healthy environment is a significant development in the protection of environmental rights. It called on states to step up efforts to ensure their people have access to a clean, healthy and sustainable environment[22]. Where as in October 2021, the United Nations (UN) Human Rights Council adopted a resolution

[18] See, Laura Van Waas: The Intersection of International Refugee Law and International Statelessness Law. In: Cathryn Costello – Michelle Foster – Jane McAdam (eds.): *The Oxford Handbook of International Refugee Law*, OUP, 2021. 152-170.

[19] Views adopted by the Committee under article 5 (4) of the Optional Protocol, concerning communication No. 3624/2019, Human Rights Committee, CCPR/C/135/D/3624/2019, 22 September 2022.

[20] CCPR/C/135/D/3624/2019, para 8.

[21] Ioane Teitiota v. New Zealand (advance unedited version), CCPR/C/127/D/2728/2016, UN Human Rights Committee (HRC), 7 January 2020, available at: https://www.refworld.org/cases,HRC,5e26f7134.

[22] A/RES/76/300, information A/76/251 74b Human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms. Human Rights Advancement, [New York]: UN, 26 July 2022.

recognizing 'the right to a clean, healthy and sustainable environment' as a 'human right that is important for the enjoyment of human rights'.[23]

This resolution could be a first step towards filling a significant gap in international law. Furthermore, although it is not legally binding, the resolution has the potential to prompt states to adopt similar measures at the national and regional levels[24]. Additionally,, the right to a healthy environment contributes to improved implementation and enforcement of climate litigation, protects against gaps in climate laws, and creates opportunities for better access to climate justice.[25]

The 1972 Stockholm Declaration on the human environment was the first international document to recognize the link between human rights and the environment[26].while the Paris Climate Agreement acknowledges in its preamble that states should, when taking action to address climate change, respect, promote and consider their respective obligations on human rights.

Remarkably, the inter-American human rights system expressly mentioned the right to a healthy environment in article 11 of the Protocol of San Salvador, which says that everyone shall have the right to live in a healthy environment and to have access to basic public services. Besides, the States shall promote the protection, preservation, and improvement of the environment.[27]

The Inter-American Court of Human Rights has demonstrated that according to the close connection between environmental protection, sustainable development and human rights, currently numerous human rights protection systems recognize the right to a healthy environment as a right in itself. It also reiterates that the human right to a healthy environment has been understood as a right that has both individual and also collective connotations. In its collective dimension, the right to a healthy environment constitutes a universal value that is owed to both present and future generations. On the other hand, the right also has an individual dimension insofar as its breach may have a direct and an indirect

[23] Human Rights Council Resolution 48/13, UN Doc A/HRC/RES/48/13 (2021) at 1.

[24] Engin Firat: Rights-based litigation in tackling climate change. Can the ECtHR be effective in protecting human rights in the context of climate change? *Law & Justice Review*, 26/2023, 89–139. 112.

[25] Pau de Vilchez Annalisa Savaresi: The Right to a Healthy Environment and Climate Litigation. A Game Changer. *Yearbook of International Environmental Law*, 1/2021, 3–19. 4.

[26] The principle 1 of declaration states: *"Man has the fundamental right to freedom, equality and adequate conditions of life, in an environment of a quality that permits a life of dignity and well-being, and he bears a solemn responsibility to protect and improve the environment for present and future generations. In this respect, policies promoting or perpetuating apartheid, racial segregation, discrimination, colonial and other forms of oppression and foreign domination stand condemned and must be eliminated".*

[27] Additional Protocol to the American Convention on Human Rights in the Area of Economic, Social and Cultural Rights (Protocol of San Salvador), entered into force November 16, 1999.

impact on the individual owing to its connectivity to other rights, such as the rights to health, personal integrity and life.[28]

In the case Earthlife Africa v Minister of Environmental Affairs, a South African non-governmental organization (NGO) filed a judicial review request challenging the government's decision to issue a license to build a coal power station. The applicants raised concerns about the power station that would significantly contribute to climate change and affect the enjoyment of human rights. The High Court of South Africa upheld the applicants' request. The court justified its decision, among other reasons, by referring to the right to a healthy environment[29].

It seems that the recognition of the human right to a healthy environment is a step in the right direction to enhance the success of human rights-based climate litigation.

In conclusion, the recognition of the fundamental human rights implicated by climate change, including the rights to life, self-determination, and access to a clean environment, highlights the urgent need for collective action and legal frameworks to address this global challenge. Recent advancements, such as the acknowledgment of the right to a healthy environment by international bodies, underscore the growing consensus on the interdependence of human rights and environmental protection. Moving forward, it is imperative for governments and stakeholders to uphold their obligations under international law, implement effective measures to mitigate climate impacts and prioritize the well-being of vulnerable communities.

3. Climate change and the law of the sea

Climate change undeniably creates new challenges for the Law of the Sea, which then must adapt to tackle its impacts. COP 26 in Glasgow referred to the integration between the law of the sea and climate change. The formal outcome of COP 26 contains several references to the oceans. As a result, it becomes imperative to understand how legal frameworks, particularly the United Nations Convention on the Law of the Sea (UNCLOS), address and adapt to these challenges.

This study explores the intersection of climate change and the Law of the Sea, delving into UNCLOS obligations, implications for maritime boundaries, the role of international tribunals, and the application of the precautionary

[28] Inter-American Court of Human Rights advisory opinion OC-23/17, para 54.

[29] Earthlife Africa v Minister of Environmental Affairs et al, High Court of South Africa Gauteng Division, Pretoria, Judgment (6 March 2017), Case number: 65662/16, para 81.

principle. Through an examination of these key areas, with aim to shed light on the evolving legal landscape surrounding climate change and its impact on marine environments.

3.1 Obligations Under the United Nations Convention on the Law of the Sea (UNCLOS)

The United Nations Convention on the Law of the Sea (UNCLOS) provides that states have the obligation to protect and preserve the marine environment, and this general obligation is affected by climate change[30]. Consequently, the violation of the obligation of protecting and preserving the marine environment could be invoked in terms of climate change under the dispute settlement mechanism provided for in Part XV of the UNCLOS[31].

The maritime boundaries delimitation remains a primary focus of the international Law of the Sea and the UNCLOS, thus shifting baselines resulting from sea-level rise due to climate change will cause a modification of the marine spaces of some coastal and archipelagic States. That will undoubtedly introduce tension between States concerning the delimitation of national maritime boundaries, access to natural resources and navigation[32].

The preamble of the Paris Agreement stated expressly the importance of ensuring the integrity of all ecosystems, including oceans and the protection of biodiversity. Although the primary does not bear binding value, it is important when it comes to interpreting the agreement positions besides the broader constellation of international legal frameworks and its relationship with other legal instruments.

Despite the fact that the UN Convention on the Law of the Sea UNCLOS is a comprehensive international legal instrument established to govern the oceans, it makes no explicit reference to climate change. Its preamble provides that its purpose is to create a legal order for the seas and oceans, which will facilitate international communication and will promote the peaceful uses of the seas and

[30] The article 192 of UNCLOS states: *"States have the obligation to protect and preserve the marine Environment."*, also article 194/1 provides: *"States shall take, individually or jointly as appropriate, all measures consistent with this Convention that are necessary to prevent, reduce and control pollution of the marine environment from any source, using for this purpose the best practicable means at their disposal and in accordance with their capabilities, and they shall endeavor to harmonize their policies in this connection"*.

[31] See, articles 279-299 of UNCLOS.

[32] Randall S. Abate: *Climate Change Impacts on Ocean and Coastal Law. U.S. and International Perspectives*. Oxford University Press, 2015. 256.

oceans, the equitable and efficient utilization of their resources, the conservation of their living resources and the study, protection and preservation of the marine environment.[33]

However, article 192 of the convention forms a general obligation to protect and preserve the marine environment[34], and the International Tribunal for the Law of the Sea (ITLOS) has elaborated on the term of 'marine environment' in its Fisheries Advisory Opinion, where it found that this includes living resources and marine life. The statement further asserts the conservation of the living resources of the sea is an element in the protection and preservation of the marine environment[35]. Although Article 192 phrased in general terms, it has been considered well established that Article 192 does impose a duty on States Parties[36].

3.2. The role of International Tribunals

International tribunals, such as the International Tribunal for the Law of the Sea, interpret UNCLOS obligations, emphasizing due diligence in protecting the marine environment and preventing future damage.

In the South China Sea Arbitration, the Permanent Court of Arbitration discussed article 192 at length affirming that the general obligation enshrined therein is one of due diligence, which extends both to protection of the marine environment from future damage and preservation in the sense of maintaining or improving its present condition[37].

[33] UNCLOS, Preamble.

[34] Article 192 stated: *"States have the obligation to protect and preserve the marine environment"*.

[35] The Advisory Opinion of the International Tribunal for the Law of the Sea on the Request submitted to the Tribunal by the Sub-Regional Fisheries Commission on 2 April 2015. It is available on the Tribunal's websites (http://www.itlos.org and http://www.tidm.org).

[36] Saint Vincent and the Grenadines v. Kingdom of Spain, Provisional Measures, Order of 23 December 2010, ITLOS Reports 2008-2010. 58.

[37] Permanent Court of Arbitration (PCA) Case No. 2013-19, in the matter of the South China Sea arbitration, – before – an arbitral tribunal constituted under Annex VII to the 1982 United Nations Convention on the Law of the Sea – between - the Republic of the Philippines – and – the People's Republic of China, 12 July 2016.
At the outset, the Tribunal notes that the obligations in Part XII apply to all States with respect to the marine environment in all maritime areas, both inside the national jurisdiction of States and beyond it. (same case law at g. Request for an Advisory Opinion Submitted by the Sub-Regional Fisheries Commission (SRFC), Advisory Opinion of 2 April 2015, ITLOS Reports 2015, para. 120) Accordingly, questions of sovereignty are irrelevant to the application of Part XII of the Convention.

Remarkably, the court also reiterated that the content of the general obligation in Article 192 requires that States ensure that activities within their jurisdiction and control respect the environment of other States or of areas beyond national control[38].

The content of the general obligation in Article 192 is further explained in the subsequent provisions of Part XII, including Article 194, which concerns pollution of the marine environment, as well as by reference to specific obligations set out in other international agreements, as envisaged in Article 237 of the Convention[39].

The International Tribunal for the Law of the Sea sheds light on the obligation of a flag State to ensure its fishing vessels not be involved in activities, which will undermine a flag State's responsibilities under the Convention in respect of the conservation of living resources and the obligation to protect and preserve the marine environment[40]. Therefore, this case law can serve as a springboard to assert that the previous articles of the convention provide a foundation for establishing an obligation to combat climate change and its causes, which likely pose a serious threat to the marine environment.

On another occasion, the court illustrated that the expression 'to ensure' is often used in international legal instruments to refer to obligations. In regard to paragraph 2 of Article 194, it adds: *"States shall take all measures necessary to ensure that activities under their jurisdiction or control are so conducted as not to cause damage by pollution to other States and their environment..."*, in which this obligation may be characterized as an obligation "of conduct" and not "of result", and as an obligation of "due diligence".[41]

[38] See, the same principle in the international court of justice law case: Legality of the Threat of Use of nuclear weapons, Advisory Opinion, ICJ Reports 1996, 226,240-242, para. 29.

[39] Article 237, entitled *Obligations under other conventions on the protection and preservation of the marine environment, states: 1. The provisions of this Part are without prejudice to the specific obligations assumed by States under special conventions and agreements concluded previously, which relate to the protection and preservation of the marine environment and to agreements which may be concluded in furtherance of the general principles set forth in this Convention.*
2. Specific obligations assumed by States under special conventions with respect to the protection and preservation of the marine environment, should be carried out in a manner consistent with the general principles and objectives of this Convention."

[40] See, Southern Bluefin Tuna (New Zealand v. Japan; Australia v. Japan), Provisional Measures, Order of 27 August 1999, ITLOS Reports 1999, 280, at 295, para. 70; Pulp Mills on the River Uruguay (Argentina v. Uruguay), the International Court of Justice Judgment, ICJ Reports 2010, 14, at 79, para. 197.

[41] Responsibilities and Obligations of States Sponsoring Persons and Entities with respect to Activities in the Area (Request for Advisory Opinion submitted to the Seabed Disputes Chamber), Advisory Opinion of 1 February 2011, ITLOS Reports 2011.

The Permanent Court of Arbitration rejected the argument that Part XII of the Convention (relating to the protection and preservation of the marine environment) are limited to measures aimed at controlling marine pollution. In the Tribunal's view, Article 194 is accordingly not restricted to measures aimed strictly at controlling pollution and extends to measures focused primarily on conservation and the preservation of ecosystems[42].

Moreover, in the South China Sea Arbitration, it is affirmed that paragraph 5 of Article 194 covers all measures under Part XII of the Convention (whether taken by States or those acting under their jurisdiction and control) that are necessary to protect and preserve "rare or fragile ecosystems" as well as the habitats of endangered species.

3.3. UNCLOS and Climate Change Mitigation

Although the provisions of Part XII, which are concerned with pollution to the marine environment, were not drafted with climate change in mind, it is well accepted that they are broad enough to encompass pollution by greenhouse gases[43]. Thus, these provisions can be applicable to climate change, since they can be interpreted so as to cover all contemporary threats to the marine environment.

The climate crisis caused by greenhouse gases meets the definition of "pollution of the marine environment" in UNCLOS Article e 1(4). The Intergovernmental Panel on Climate Change (IPCC) has reported extensively on the adverse impacts of climate change on the marine environment[44]. The world's oceans have absorbed more than 90% of the additional energy trapped by the greenhouse effect and approximately 30% of anthropogenic carbon dioxide from the atmosphere[45]. This absorption has heated, deoxygenated, and acidified the marine environment.[46]

[42] The Permanent Court of Arbitration, Chagos Marine Protected Area Arbitration (Mauritius v. United Kingdom), Award, 18 March 2015, paras. 320, 538.

[43] Karen N. Scott: Ocean Acidification. In: Elise Johansen – Signe Veierud Busch – Ingvild Ulrikke Jakobsen (eds.): *The Law of the Sea and Climate Change. Solutions and Constraints.* Cambridge University Press, 2021. 113.
Alan Boyle: Litigating Climate Change under Part XII of the LOSC. *-The International Journal of Marine and Coastal Law*, 3/2019, 458–481. 462.

[44] IPCC, AR6 Synthesis Report of the IPCC Sixth Assessment Report: Climate Change 2023, paras B.1.4, B.2.1.

[45] IPCC, Report of Working Group I (Physical Science Basis), AR6: Summary for Policymakers, A.4.2; IPCC Working Group II, AR5, 1658.

[46] Ocean temperatures were 0.88°C [0.68°C-1.01°C] higher in 2011-2022 than in 1850-1900. IPCC (2023) AR6, Summary for Policymakers, pg. 4.

Another reasonable point argues that climate crisis-related pollution of the marine environment threatens the right to life. Therefore, in the case of Billy v. Australia, the UN Human Rights Committee examined whether Australia's alleged failure to protect complainants from the effects of climate change amounted to a violation of Australia's obligations under Article 6 of the International Covenant on Civil and Political Rights[47].

The Committee revealed that under those circumstances, the pollution of the marine environment resulting from greenhouse gas emissions threatens the right to life. Thus, States have an obligation to take effective measures to mitigate climate change, strengthen the adaptive capacity of vulnerable populations and prevent foreseeable loss of life[48].

Not only does the climate crisis-related pollution of the marine environment threaten the human right to a clean, healthy and sustainable environment, but it also compromises access to food. The UN Special Rapporteur on the Environment has observed that Pollution of the marine environment affects fisheries and consequently threatens the right to food[49].

According to article 212 of UNCLOS, States focus on the duty of states to cooperate in the prevention of global atmospheric pollution. This obligation complements with the general obligation stated in articles 193 and 194(1) to "protect and preserve the marine environment" and to "prevent, reduce and control pollution of the marine environment from any source". These provisions collectively reflect the commitment of states to reduce their greenhouse gas emissions under UNCLOS.

The precautionary principle is a key concept in international environmental law[50]. As a result, the Second Chamber of ITLOS has mentioned expressly the Seabed Disputes in its advisory opinion that there is a trend to put this principle besides customary international law and its enforcement may be required in

47 See Billy v. Australia, CCPR/C/135/D/3624/2019.

48 Human Rights Committee, General Comment No. 36, CCPR/C/GC/36, 3 Sept. 2009, para. 62.

49 In the oceans, temperature changes, bleaching of coral reefs and ocean acidification are affecting fisheries. Climate change also exacerbates drivers of food insecurity and malnutrition, such as conflict and poverty.
See, Report of the Special Rapporteur on the issue of human rights obligations relating to the enjoyment of a safe, clean, healthy and sustainable environment, United Nations High Commissioner for Human Rights, A/74/161, 15 July 2019. Available at www.ohchr.org/EN/Issues/Environment/SREnvironment/Pages/Annualreports.aspx.

50 It involves that where they are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation. See: Rio Declaration on Environment and Development 1992, Principle 15.

light of article 31, paragraph 3(c) of Vienna Convention on the Law of Treaties.[51] Therefore, states must adopt a precautionary approach to activities that may pollute the marine environment through the emission of greenhouse gases.

Although climate change is not expressly referred to in UNCLOS, its adverse effects on the ocean are to be considered as 'pollution' under the terms of Article 1(1)(4), regardless of the source. Therefore, the provisions of Article 194 to prevent, reduce and control those effects apply along with the following obligations established by Part XII.

In contrast to UNCLOS, which makes no explicit reference to climate change, the Agreement under the United Nations Convention on the Law of the Sea on the Conservation and Sustainable Use of Marine Biological Diversity of Areas beyond National Jurisdiction[52] has recognized the need to address biological diversity loss and the degradation of the ecosystems of the ocean in a coherent and cooperative manner, in particular, to climate change impacts on marine ecosystems, such as warming and ocean deoxygenation, as well as ocean acidification, pollution, including plastic pollution, and unsustainable use.Remarkably, when the agreement identified the term of cumulative impacts, it elaborated that it means the combined and incremental impacts resulting from different activities, including the consequences of climate change[53]. Thus, climate change impacts are considered in the conduct of environmental impact assessments (EIAs), as States are under an obligation to take cumulative impacts into account, when conducting EIAs.[54]

It is important to emphasize the fundamental principle of international law regarding the duty to cooperate, a principle that lies at the core of the United

[51] Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area (Request for Advisory Opinion Submitted to the Seabed Disputes Chamber), Case No. 17, Advisory Opinion of Feb. 1, 2011, 17 ITLOS, para 135.
Article 31, paragraph 3(c) of Vienna Convention states that the interpretation of a treaty should take into account not only the context but *"any relevant rules of international law applicable in the relations between the parties"*.

[52] The Agreement was adopted in New York on 19 June 2023 during the further resumed fifth session of the Intergovernmental conference on an international legally binding instrument under the United Nations Convention on the Law of the Sea on the conservation and sustainable use of marine biological diversity of areas beyond national jurisdiction. The Agreement shall be open for signature in New York on 20 September 2023 and shall remain open for signature until 20 September 2025.

[53] See, article 1 para 6.

[54] Article 27 of the agreement affirmed that the provisions of the Convention on environmental impact assessment for areas beyond national jurisdiction needed to implement by establishing processes, thresholds and other requirements for conducting and reporting assessments by Parties.

Nations Charter (Articles 1.3 and 56), reflected in numerous international instruments (Rio Declaration and Tokyo Protocol as well as ICESCR arts 2, 11, 15, 22 and 23). In the case of environmental disasters, States must strengthen international cooperation among themselves and assist, prevent, avoid and respond to all types of risks with relevant international organizations and agencies.

4. Conclusion

As a summary, the intertwining of climate change with international law, particularly in the realms of human rights and the Law of the Sea, highlights the urgent need for global cooperation and action. The recognition of basic human rights, such as the right to life and a healthy environment, underscores the interconnectedness of climate change and the protection of vulnerable communities. Recent developments, including the acknowledgment of the right to a healthy environment by international bodies, signify progress in addressing the harmful effects of climate change on human well-being.

Within the framework of the Law of the Sea, the United Nations Convention on the Law of the Sea (UNCLOS) serves as a crucial tool for regulating ocean activities and addressing emerging challenges, including those posed by climate change. Despite UNCLOS's silence on climate change, its provisions on marine environmental protection provide a foundation for mitigating climate-related impacts on marine ecosystems.

International tribunals, such as the International Tribunal for the Law of the Sea, play a vital role in interpreting UNCLOS obligations and ensuring compliance with international law. Through their rulings and advisory opinions, these tribunals contribute to shaping legal frameworks that support sustainable ocean governance and climate change mitigation.

Moving forward, it is essential for governments, stakeholders and the global community to fulfill their responsibilities under international law, implement effective measures to address climate impacts and prioritize the welfare of vulnerable populations. By fostering collaboration, strengthening legal frameworks, and promoting sustainable practices, we can collectively confront the multifaceted challenges posed by climate change and protect the rights and resources of current and future generations.

Bibliography

Amy Maguire – Jeffrey McGee: A Universal Human Right to Shape Responses to a Global Problem? The Role of Self-Determination in Guiding the International Legal Response to Climate Change. *Review of European Community and International Environmental Law*, 1/2017.

Benoit Mayer: The Contribution of Urgenda to the Mitigation of Climate Change. *Journal of Environmental Law*, 2/2023, 167–184.

Curt D. Storlazzi et al.: Most Atolls Will Be Uninhabitable by the Mid21st Century Because of Sea-Level Rise Exacerbating Wave-Driven Flooding. *Science Advances*, 4/2018.

Etienne Piguet: Climatic Statelessness: Risk Assessment and Policy Options. *Population and Development Review*, 4/2019, 865–883.

Laura Van Waas: The Intersection of International Refugee Law and International Statelessness Law. In: Cathryn Costello – Michelle Foster – Jane McAdam (eds.): *The Oxford Handbook of International Refugee Law*, OUP, 2021. 152-170.

Engin Firat: Rights-based litigation in tackling climate change. Can the ECtHR be effective in protecting human rights in the context of climate change? *Law & Justice Review*, 26/2023, 89–139.

Pau de Vilchez Annalisa Savaresi: The Right to a Healthy Environment and Climate Litigation. A Game Changer. *Yearbook of International Environmental Law*, 1/2021, 3–19.

Randall S. Abate: *Climate Change Impacts on Ocean and Coastal Law. U.S. and International Perspectives*. Oxford University Press, 2015.

Karen N. Scott: Ocean Acidification. In: Elise Johansen – Signe Veierud Busch – Ingvild Ulrikke Jakobsen (eds.): *The Law of the Sea and Climate Change. Solutions and Constraints.* Cambridge University Press, 2021.

Alan Boyle: Litigating Climate Change under Part XII of the LOSC. -*The International Journal of Marine and Coastal Law*, 3/2019, 458–481.

GOOD CORPORATE GOVERNANCE. BEST PRACTICE TOOL TO SAFEGUARD THE NON-PROFIT COMPANIES FROM ABUSING FOR FUNDING TERRORISM. THE CASE OF JORDAN

Raghad Al-Shareedah[1]

ABSZTRAKT ■ Ez a tanulmány az egyik legjobb nemzetközi gyakorlatra összpontosít, amely a nonprofit szektort a terrorista visszaélésektől védi: a jó vállalatirányítási intézkedésekre a jordániai kontextusban. Jordánia jelentős előrelépést tett a nonprofit szektor védelmében a terrorizmusfinanszírozási célúvisszaélésekkel szemben, mind a jogszabályok, mind a technikai reformok terén. Azonban ez a fejlődés nem lehet teljes a vállalatirányítási elvek elfogadása nélkül. A jordániai jogszabályok szerint a vállalatirányítási szabályok végrehajtása kötelező az 500 000 jordániai dínárt meghaladó jegyzett tőkével rendelkező magán részvénytársaságokra, valamint a nyilvános részvénytársaságokra, de nem kötelező a korlátolt felelősségű társaságokra. Az ilyen megfelelőség alapvető fontosságú a globális terrorizmus elleni harcban, és egyben lépést jelent az NPC szektor integritásának megőrzése felé.

ABSTRACT ■ This paper will concentrate on one of the International best practices to safeguard the nonprofit industry from terrorist misuse: good corporate governance measures within the Jordanian context. Jordan has made a very well-noticed advancement in the issue of protecting the non-profit sector from abusing for funding terrorism, in terms of legislation and technical reforms. Still, such progress cannot be completed without adopting corporate governance principles. According to Jordan's legislation, implementing corporate governance rules is binding to registered Private Shareholding companies with subscribed capital exceeding JOD. 500000 and registered Public Shareholding but non-binding for Limited Liability Companies. Such compliance is essential to the worldwide war on terror and a step toward maintaining the NPC sector's integrity.

1. Why Non-Profit Companies?

A typical aspect of many non-profit theories is their focus on the service-providing functions of non-profit organizations, while often overlooking their

[1] PhD Student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

role in redistribution. Simplifying somewhat, there are two potential public policy approaches to addressing social inequalities: (1) the welfare state model, where the government controls and manages welfare redistribution; and (2) the non-profit-based model, which involves a large network of private organizations heavily backed by the government, along with additional services provided by the government.[2]

The non-profit sector is a major employer and serves as an effective tool for mobilizing public resources. They play a significant role in social development across all areas and provide various services and conduct research in vital fields such as health, education, scientific advancement, and local development. They are considered part of civil society, which includes a range of voluntary, civil, and social organizations that complement the legislative, administrative, and judicial authorities supported by the government. NGOs offer people of all ages diverse perspectives and opportunities to express their views, highlight community problems, and unite those with shared convictions to achieve common goals through volunteering, discussion, dialogue, and good deeds.[3]

The financial and economic sustainability of the non-profit sector relies on a system that ensures the continuous and efficient acquisition and utilization of resources through strategic planning. This planning outlines the organization's objectives, the methods to achieve them, and evaluates the current performance of these organizations and their ability to adapt to changing circumstances.[4]

FATF's concentration on the Non-Profit Organizations (NPOs) sector lies on several reasons as they might frequently operate with minimal or no governmental supervision, such as in the aspects of registration, record-keeping, reporting, and monitoring. The creation of NPOs may involve few formalities, such as lacking prerequisites for skills or starting capital, and may not mandate background checks for employees. Exploiting these characteristics, terrorist organizations have capitalized on the vulnerability of NPOs, infiltrating the sector and misusing their funds and operations to camouflage or facilitate terrorist activities.[5]

[2] Éva Kuti: The Possible Role of the Non-Profit Sector in Hungary. *Voluntas: International Journal of Voluntary and Nonprofit Organizations*, 1/1990, 26–40. 26. http://www.jstor.org/stable/27927272. Accessed 18 July 2024.

[3] Ismail Al Zyoud: The Role of Non-Governmental Organizations in Development of Jordanian Society. *Dirasat: Human and Social Sciences*, 1/2019.

[4] RASHEED TI-JO, CSOs and NGOs. Ways of Financial Sustainability. Rasheed TI-JO Research Series: Third Sector. Vol.2. 2020.

[5] FATF, IX Special Recommendations. Paris, 2001. . https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf.coredownload.pdf.

As stated in the interpretive note accompanying recommendation (8), terrorists and terrorist groups may utilize certain non-profit companies (NPCs) within the sector for purposes such as fundraising, facilitating the movement of funds, providing logistical assistance, recruiting individuals for terrorist activities, or otherwise supporting terrorist organizations and their operations. This exploitation not only enables terrorist actions but also undermines donor trust and jeopardizes the fundamental integrity of NPCs.

1.1. Non-Profit Companies Definition

For the implementation of recommendation (8), FATF adopted a definition applied to the legal entities or arrangements primarily involved in raising or disbursing funds for charitable, religious, cultural, educational, social, fraternal purposes, or other forms of "good works" (referred to as the "FATF definition").[6]

Such a definition does not encompass the entire spectrum of not-for-profit entities. They vary in their susceptibility to terrorism financing abuse based on their types, activities, or characteristics, with the majority likely presenting a low risk.

All member states to FATF shall specify all companies that fall under the definition of FATF and use all related information to specify the types and characteristics that may expose the non-profit companies for abuse due to the nature of businesses, the nature of threats, and how the terrorists' abuse of non-profit companies shall be defined.

FATF's definition applies to non-profit companies (NPC) under the supervision of the Companies Control Department (CCD) in Jordan. Only companies carrying out businesses in the health sector, education sector, microfinance, investment promotion, training, or any other objective in the form of limited liability or private shareholding general partnership, or limited partnership company are registered in the records of CCD.

Nevertheless, the Jordanian legislator did not provide a specific definition for non-profit companies according to the Companies Law No. (22) of 1997 and its amendments, the Non-Profit companies can be defined according to article (2), paragraph (B) of non-profit company's regulation No. (73) for the year (2010) as companies, which do not aim to achieve any profit and if it has achieved any returns, it is not permissible to distribute it to any of the companies or its shareholders.[7]

[6] FATF, BPP-Combating the Terrorist Financing Abuse of Non-Profit Organisation. Paris, 2023.

[7] Companies law and its amendments, 22, 1997. https://ccd.gov.jo/EBV4.0/Root_Storage/AR/r_Folder_/%D9%82%D8%A7%D9%86%D9%88%D9%86_%D8%A7%D9%84%D8%B4%D8%B1%D9%83%D8%A7%D8%AA_%D9%85%D8%B9%D8%AF%D9%84.pdf.

1.2. Non-Profit Companies in Jordan

In Jordan, NGOs play a crucial role in supporting the government's developmental efforts, especially for disadvantaged groups of the population. Such firms may exist in various structures, such as a sole proprietorship (including personal charitable donations), an unincorporated association, a corporation, a foundation (characterized by its funding from a founder and organized as a trusteeship), or a condominium.

According to department of statistics in Jordan for the year 2016, this sector constitutes 1% in the GDP as sectoral contribution to the Jordanian Economy.[8]

The Companies Law No. (22) of 1997 and its amendments allow, under Article (7/d), the registration of non-profit companies including, General Partnership, Limited Partnership, Limited Liability and Private Shareholding companies to carry out health, education, microfinance, investment promotion, and training, and other objectives aimed at community development, or any related purpose approved by the Controller.[9]

The law also regulates general provisions related to registration, management, holding meetings, obtaining financing, liquidation, and more. Furthermore, the Regulation of Non-Profit Companies No. (73) of (2010) lays out detailed rules for such companies' establishment, the conditions under which they may operate, and other related matters such as supervision and oversight, the methods and procedures for obtaining aid and donations, their sources of funding, the method of spending, liquidation procedures, and the handling of their funds upon liquidation.

It also outlines the data these companies must submit to the Companies Control Department, as well as the conditions and procedures for transforming them into or from profit companies.[10]

2. Mechanisms of Misusing Non-Profit Companies to Fund Terrorism

Terrorist organizations to conceal or support their terrorist activities have been able to exploit the characteristics the Non-Profit organizations enjoy such as gaining public trust and having substantial sources of revenue. Additionally, some non-profit organizations have a global presence that provides a framework to conduct their businesses locally and internationally, often in or near areas most susceptible to terrorist activity.

8 Jordan Economic Growth Plan 2018 – 2022-the economic policy council, Amman-Jordan.
9 Governance guidelines for non-profit companies, 2021.
10 Ibid.

A set of factors that may create vulnerabilities, increasing the exposure of non-profit organizations to the risks of terrorist financing including but not limited to geographical expansion, the nature of businesses and non-compliance with corporate governance principles, etc.

2.1. Geographical Threats

The more an organization expands the scope of its activities, beneficiaries, and geographical locations through which it gathers, retains, transfers, and delivers financial or material resources, the greater the risk of exploitation. Organizations that work intensively in multiple activities and across wide geographical areas, especially when material or financial resources cross regions lacking oversight and governance or when they operate in conflict zones, are particularly vulnerable. [11]

2.2. The Nature of Companies' Activities

There is a relationship between the nature of activities carried out by an organization and the risks of terrorism financing. Non-profit organizations that engage in service activities, specifically "humanitarian aid organizations", which provide services such as housing, poverty alleviation, education, or healthcare, are more susceptible to the risks of terrorism financing. However, the level of exposure to these risks varies. Organizations operating near or within areas where terrorist groups are present are at higher risk compared to others. Additionally, organizations working in vulnerable and exploitable communities (such as refugees, for example) are at greater risk of terrorism financing, as they become targets that terrorist groups seek to exploit or control.[12]

2.3. Non-Compliance with Corporate Governance Principles

The absence of adopting sound governance rules and strong financial management weaken the organization or company and increase its exposure to exploitation to terrorism financing. Non-profit organizations should be established according to a formal document governing their framework (such as the Articles of Association,

[11] The Register of Associations, the Companies Control Department, the Anti-Money Laundering and Counter-Terrorism Financing Unit. How to safeguard your organizations from the risks of terrorism funding, 2022.

[12] Ibid.

a constitution, or internal regulations) that defines their purposes, structure, reporting practices, and compliance with local laws. Additionally, it is crucial that board members have a deep understanding of the organization's goals and act in its best interests. The board of directors should maintain oversight of the organization by implementing robust financial and human resource policies, meeting regularly, and closely monitoring activities.[13]

Moreover, establishing robust financial controls and procedures is essential to prevent non-profit organizations from financial misconduct and misuse of resources and funds. For example, the board of directors approves the annual budget and implements a process for monitoring the use of funds. Non-profit organizations must maintain sufficient and complete financial records of revenues, expenditures, and financial transactions throughout their operations, including the final use of funds. They should clearly define program objectives when raising funds and ensure that the funds are used as intended. Additionally, information about the activities carried out should be made available to the public, and the organization may establish criteria for determining whether to accept or reject donations.[14]

3. Corporate Governance as a Best Practice Tool to Safeguard the Non-Profit Companies from Exploitation for the Purposes of Funding Terrorism

To prevent terrorists or criminals from exploiting the non-profit organizations, it is important for these organizations to have strong financial controls and to be transparent in their activities. It is advisable for non-profit organizations to conduct regular reviews of their internal controls, policies, procedures, key programs, and partnerships to protect themselves from actual or perceived misuse or support of terrorism. One of the practices that can be followed to mitigate the risks of terrorist financing is implementing corporate governance principles.

3.1. What is Corporate Governance?

The literature on corporate governance has included numerous definitions of the subject, and there has not yet been a consensus on a specific definition.

[13] Ibid.
[14] Ibid.

However, despite the variety of definitions, they all adhere to the basic principles that governance involves: a set of procedures, norms, policies, and laws that influence the way a company is managed transparently, monitor its management, and impose a fair balance among the parties involved in the company's operations.[15]

According to the Cadbury Report (1992), corporate governance is defined as the system through which companies are directed and controlled. It entails balancing the interests of various stakeholders, including shareholders, management, customers, suppliers, financiers, government, and the community.[16]

Corporate governance broadly refers to how a firm's key components are structured, coordinated, and motivated to achieve common objectives and adapt to change. It primarily involves defining and distributing decision-making authority and control within the firm, determining who makes which decisions. This, in turn, affects how residual income is allocated. Decision-making power involves rights (such as property rights) and responsibilities, which can be established through contracts or other means (e.g., reputation, tradition, or coercion). Effective governance must go beyond decision-making to also address motivations, incentives, organization, coordination of stakeholders, and the process of managing change.[17] Corporate governance focuses on whether the leaders of a company are held accountable for how they exercise their powers and how risks are managed.[18]

The primary areas addressed by corporate governance codes include the role and responsibilities of the board of directors and ensuring they are properly executed. The B.O.D. shall have a clear understanding of their duties, fulfilling these responsibilities, and providing effective leadership for the company. The board must be accountable to its shareholders and transparent with investors. Governance focuses on key areas involving risk management, internal control, financial reporting, narrative reporting and auditing.

In Jordan's corporate governance rules for Shareholdings and Limited Liability Companies for the year 2012, corporate governance is defined as a system by which a company is managed and overseen. The governance framework defines

[15] Mohamed Jaffer – Syed Sohail: "Corporate governance issues in Family owned Enterprises." Published by CIPE, available on this site www.cipe.org(blog.p2.).

[16] Cadbury Committee, 1992.

[17] Bruno Dallago: Corporate Governance and Governance Paradigms. *Journal of Economics and Business*, 2/2002, 173–196. 174-175.

[18] https://portal.abuad.edu.ng/lecturer/documents/1538629670Concept_of_Corporate_Governance.pdf.

the distribution of responsibilities and roles among the various participants in the company as the shareholders, the B.O.D., the management and the stakeholders.

3.2. Corporate Governance Principles

Recommendation (8) set out by FATF states that "*Countries should review the adequacy of laws and regulations that relate to non-profit organisations which the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused and proportionate measures, in line with the risk based approach, to such non-profit organisations to protect them from terrorist financing abuse, including: (a) by terrorist organisations posing as legitimate entities; (b) by exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and (c) by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.*"[19]

One of the OECD principles is ensuring the basis for an effective corporate governance framework and this can be ensured through supervisory, regulatory, and enforcement authorities, which must possess the authority, autonomy, integrity, resources, and capacity to carry out their duties in a professional and objective manner. Their decisions should be timely, transparent, and thoroughly explained.[20]

This autonomy should be paired with high ethical standards and accountability mechanisms, ensuring decisions are timely, transparent, and open to public and judicial scrutiny. As the number of corporate events and disclosures grows, the resources of supervisory, regulatory, and enforcement authorities may become strained, increasing the need for fully qualified staff to provide effective oversight and investigative capacity, which will require sufficient funding. Many jurisdictions address this by imposing levies on supervised entities as a means to ensure financial independence from government funding while maintaining transparency in how these fees are determined. Attracting staff on competitive terms is also crucial to enhancing the quality and independence of supervision and enforcement.

On Jordan's level, the adoption of a risk-based approach is also required and for the purposes of conducting the said approach, a team was formed in 2022 in

[19] FATF, Combating the abuse of Non-Profit organizations (recommendation 8). Paris, 2015. https://www.fatf-gafi.org/media/fatf/documents/reports/BPP-combating-abuse-non-profit-organisations.pdf.

[20] OECD, G20/OECD Principles of Corporate Governance 2023. OECD Publishing, Paris, 2023. https://doi.org/10.1787/ed750b30-en.

order to define the threats and vulnerabilities of exposing to risks of misusing to fund terrorists to all legal persons. At the same time the approach targeting non-profit companies was prepared in 2022 by a committee that was formed to classify the non-profit organizations to certain characteristics resulting from intensive investigation to the sector concluded with the level of vulnerability threats facing the companies, which is low.

The committee did consider the following criteria to steer the authority responsible for supervising the Non-Profit Companies when identifying which of them is exposed to risks which of them has a level that is high, medium or low and help them to set up effective frameworks:

1. Does the company operate in areas with high unemployment rates?
2. Does the company operate in areas with high poverty rates?
3. Does the company operate in areas prone to natural disasters?
4. The extent of the organization's activities within the Kingdom. As previously mentioned, geographical expansion within the Kingdom is a factor that increases risks, especially if the expansion includes border areas or areas that host refugee communities.
5. The extent of the organization's activities outside the Kingdom. Expansion outside the Kingdom is considered a factor that increases risks, especially if the areas involved are conflict zones where terrorist groups are present or in control.

The level of corporate governance in the Non-Profit companies in Jordan is above average as the instructions are non-binding for Limited liability but binding for Shareholdings Companies. Moreover, they might frequently operate with minimal or no governmental supervision in terms of their election of committees carrying out the roles of defining risks and assessing them and setting up strategies to mitigate these risks. Furthermore, the lack of obliging the staff to abide by the companies' controls and hold them accountable of misconduct. In Non-Profit Companies, implementing an internal control system and risk management framework is crucial for any Company integrity strategy. These systems play a key role in minimizing the risk of abuse, while also ensuring that governments operate efficiently to deliver programs that benefit citizens. Moreover, such policies and processes promote value for money and support effective decision-making. When well-established, they enable governments to balance enforcement with preventive, risk-based approaches.[21]

[21] OECD, Risk management. In: *OECD Public Integrity Handbook*. OECD Publishing, Paris, 2020. https://doi.org/10.1787/ebbed075-en.

Another principle set out by OECD is sustainability and resilience, which can be achieved when the Boards assess whether the company's capital structure is compatible with its strategic goals and its associated risk appetite to ensure it is resilient to different scenarios. Moreover, the corporate governance framework should ensure that boards thoroughly consider material sustainability risks and opportunities as they carry out their key responsibilities in reviewing, monitoring, and guiding governance practices, disclosures, strategies, risk management, and internal control systems, including those related to climate-related physical and transition risks.

Here comes the importance of the Board of Directors which is another corporate governance principle of the OECD. The Board of Directors have a significant role together with the shareholders and the management to fulfill legal duties that obligate them to act in their best interests.

Corporate governance refers to relationships between a company's management, its board of directors, shareholders, and other stakeholders. It establishes and defines the responsibilities of the company's managers and executives toward these stakeholders.[22]

The board plays a critical role in ensuring that effective governance and internal controls are in place to enhance the reliability and credibility of sustainability-related disclosures. They should carry out certain key functions to provide a strong internal control and risk management system, including reviewing and assessing risk management policies and procedures, establishing the company's risk appetite and culture, and overseeing its risk management, including internal controls. This involves monitoring responsibilities for managing risks, defining the types and levels of risk the company is willing to accept in pursuing its goals, and managing risks arising from its operations and relationships. The board's oversight offers essential guidance to management for handling risks to align with the company's desired risk profile.

In carrying out these functions, the board should ensure that material sustainability issues are addressed. To enhance resilience, boards should also ensure that their risk management frameworks have adequate processes for managing significant risks.

Effective management of terrorist financing risks necessitates proper governance arrangements and in particular, the board of directors are required to approve and oversee policies for risk management, and compliance. The board should have a clear understanding of the information related to financing terrorism risk assessments which should be communicated to them in a timely,

[22] ABOU-EL-FOTOUH H. (N.D.), Importance Of Corporate Governance For SMEs, 2010.

complete, understandable, and accurate manner to enable conscious decision-making.

Internal control and risk management encompass a variety of measures designed to prevent, detect, and address misuse. These measures include policies, practices and procedures that guide management and staff in safeguarding integrity by properly assessing risks and developing controls based on those risks. Equally important are the mechanisms to address corruption and breaches of integrity standards within an integrated internal control system.[23]

To support the board in overseeing risk management, some companies have established a risk committee or expanded the role of the audit committee, in response to regulatory requirements or evolving risk landscapes. The OECD's due diligence standards on responsible business conduct can also assist companies in identifying and addressing environmental and social risks and impacts from their operations and supply chains.[24]

4. The Role of the Board of Directors concerning Jordanian Legislation

One of the responsibilities of the Boards is oversight and accountability which should be clear. Emanating from OECD corporate governance principles, the boards need to consider forming specialized committees to assist them in executing their functions, particularly an audit committee or an equivalent body to oversee disclosure, internal controls, and audit-related matters. Other committees, such as those focused on remuneration, nomination, or risk management, may also support the board depending on the company's size, structure, complexity, and risk profile. The mandate, composition, and procedures of these committees should be clearly defined and disclosed by the board, which retains ultimate responsibility for the decisions made.[25]

For companies where the size, structure, sector, or development level justifies this, the use of committees can enhance the board's effectiveness by allowing a more focused approach to specific areas. The market needs to have a clear understanding of each committee's mandate, scope, working procedures, and composition. This transparency is crucial in jurisdictions where independent audit committees are required to oversee external auditor relationships. Audit committees should also monitor the effectiveness and integrity of the internal control system, which may include the internal audit function.

[23] OECD 2020.
[24] OECD 2023.
[25] Ibid.

Many jurisdictions have binding rules for independent audit committees and recommend nomination and remuneration committees on a "comply or explain" basis. While risk committees are often mandated for financial sector companies, some jurisdictions also regulate risk management for non-financial companies, either assigning this responsibility to the audit committee or to a dedicated risk committee. Separating audit and risk committee functions can be beneficial to address a broader range of risks and prevent the overload on the audit committee, allowing more time for managing risk issues.

The decision to establish additional committees should be at the company's discretion, tailored to the needs of the board. Some boards have created sustainability committees to advise on social and environmental risks, opportunities, goals, and strategies, including climate-related issues. Others have formed committees to handle digital security risks and digital transformation. Ad hoc or special committees may also be set up for specific needs or corporate transactions. Disclosure does not need to cover committees dealing with confidential commercial matters. Established committees should have access to necessary information, adequate funding, and the ability to consult external experts.[26]

In Jordan, companies are typically organized under a one-tier board system. The average board size is (7) members for limited liability, whereas for private shareholding, the number of members is specified in the article and memorandum of association.

Listed companies as Public Shareholding companies and non-listed companies as private shareholding companies registered with a capital exceeding JOD 500,000 are required to establish an audit committee composed of independent members with knowledge and experience in finance and accounting and another committee as remunerations as stipulated in article (6,7,8) of the Shareholding companies' governance instructions for the year 2024. Article (9) of the said instructions states that the mentioned companies can form other committees and shall define their mandates and the duration of their term. These fiduciary duties will be undermined if they are not required from the Limited Liability companies and most of the registered non-profit companies are of this type.

5. Implications of Adopting Corporate Governance Principles

Past corporate governance scandals (such as when Enron filed for bankruptcy in 2001 after manipulating its accounts, and WorldCom, which collapsed in 2002,

[26] Ibid.

admitted to accounting fraud, leading to the conviction and imprisonment of its CEO and Risk management and internal control ensured that the company operates within acceptable risk levels. Directors must implement an internal control system to ensure that the company's resources are used appropriately and its assets are safeguarded.[27]

Well-crafted corporate governance policies are instrumental in supporting broader economic goals and delivering three key public policy benefits. First, they assist companies in securing financing, especially from capital markets, which in turn drives innovation, productivity, and entrepreneurship, contributing to overall economic vitality. For investors, whether direct or indirect, good corporate governance provides confidence that they can engage in and benefit from the company's value creation on fair and equitable terms. Consequently, it influences the cost at which companies can obtain capital for growth.[28]

Well-crafted corporate governance policies provide a structure to safeguard investors, including households with savings invested in the market. By establishing procedures that enhance the transparency and accountability of board members and executives to shareholders, these policies help build trust in the markets, thereby facilitating corporate access to finance. A significant portion of the public invests in equity markets, either directly as retail investors or indirectly through pension and investment funds. Offering a system that ensures their rights are protected while allowing them to share in corporate value creation gives households access to investment opportunities that can potentially yield higher returns on their savings and retirement funds. As institutional investors increasingly allocate a large portion of their portfolios to foreign markets, investor protection policies should also extend to cross-border investments.[29]

Well-designed corporate governance policies contribute to the sustainability and resilience of corporations, which, in turn, can enhance the sustainability and resilience of the broader economy. Investors are increasingly considering not just companies' financial performance but also the financial risks and opportunities arising from broader economic, environmental, and societal challenges, as well as companies' resilience in managing those risks. In some regions, policymakers also focus on how companies' operations can help address these challenges. A robust corporate governance framework concerning sustainability issues can help companies recognize and respond to the interests of shareholders and other stakeholders, contributing to their long-term success. This framework

[27] https://portal.abuad.edu.ng/lecturer/documents/1538629670Concept_of_Corporate_Governance.pdf.

[28] OECD 2023.

[29] Ibid.

should include the disclosure of reliable, consistent, and comparable material sustainability-related information, including data related to climate change. In some instances, jurisdictions may define sustainability-related disclosure and materiality in terms of standards that specify the information a reasonable shareholder needs to make informed investment or voting decisions.[30]

6. Status in Jordan

The operations of non-profit companies in Jordan are governed by legislative frameworks, specifically the Companies Law No.)22(of 1997 and its amendments, as well as the Regulation of Non-Profit Companies No. (73) of 2010. These frameworks can assist companies in implementing governance by relying on legal structures.

In Jordanian legislation, the third sector faces limitations on receiving financial support, with common funding sources including grants, donations, sponsorships, business support, and membership fees. Other sources of funding, such as subsidies and entrepreneurial activities, are restricted by the country's legal framework, and financial mechanisms like allowances, state service procurement, agreements, and government contracts are rarely practiced.

Non-profit companies are subject to continuous monitoring and evaluation of their work and the projects they implement, in addition to the fact that the necessary licensing procedures are carried out in partnership with several entities.[31]

For example, sources of obtaining funds to carry out activities in any areas by the Non-Profit Companies are vulnerable to exploitation to facilitate the movement of terrorists' funds. A non-profit entity is allowed to receive funding from non-Jordanians, but must obtain the approval of the Council of Ministers with a notification showing this donation or financing, its amount, method of receiving it, the purpose for which it will be spent, and any special conditions for it[32] according to article (7/d/4) of effective Jordan's Company law.

For that purpose, a Committee for Reviewing Foreign Funding Requests was formed to work with the Foreign Funding Unit at the Ministry of Planning and

[30] Ibid.

[31] https://www.alaraby.co.uk/economy/%D8%B6%D8%A8%D8%B7-%D8%AA%D9%85%D9%88%D9%8A%D9%84-%D8%A7%D9%84%D8%B4%D8%B1%D9%83%D8%A7%D8%AA-%D8%BA%D9%8A%D8%B1-%D8%A7%D9%84%D8%B1%D8%A8%-D8%AD%D9%8A%D8%A9-%D9%81%D9%8A-%D8%A7%D9%84%D8%A3%D8%B1%D8%AF%D9%86.

[32] Ibid.

International Cooperation of Jordan to improve the alignment of foreign funding projects with national priorities and the needs of impoverished areas. They also aim to streamline the approval process for receiving funding within specified timeframes, while enhancing mechanisms to evaluate and monitor funding to ensure it aligns with its goals and assesses its impact on targeted entities.

The government has introduced new amendments to the foreign funding acquisition process, aiming to expand its scope to include associations and cooperative unions and to make funding requests automatic. These amendments are intended to refine the process, ease procedures, and broaden its application to include associations, cooperative unions, and any requests submitted to the committee from the Prime Minister's Office.

New technical and financial criteria have been adopted to evaluate foreign funding requests in line with best international practices, aligning with national developmental priorities to ensure participation and integration between the government, civil society organizations and donor entities from friendly countries and the international community.

Such governmental measures implemented over the past few years have reduced distortions and imbalances in foreign funding for civil society organizations in Jordan. According to official estimates, the amount of foreign funding received by non-profit companies and associations has decreased to around $71 million annually.[33]

Furthermore, Article (9) of the mentioned law mandates that within three months of the start of a new fiscal year, these organizations must submit an annual report to the government regulatory body (the Companies Controller Department and the relevant Ministry). This report must include details of the activities carried out, a list of funding sources, a budget certified by the organization's authorized signatories, an audit report, and any additional information requested by the controller. The organization is also required to submit a business plan outlining expected activities for the year, along with detailed information on the financing sources for those projects and programs. Additionally, they must maintain records of meetings, decisions made, and evaluations of activities, including their revenues and expenditures.

According to the latest data released by the Ministry of Planning and International Cooperation, Foreign funding consistently raises objections, as it is viewed as there is a concern that some donors may have specific goals they aim to achieve through such funding.

[33] Ibid.

According to the Ministry of Planning and International Cooperation website, the amount of foreign funding provided to associations, non-profit companies, unions, and cooperative societies that received Cabinet approval for the year (2024) reached approximately 25.4 million dinars during the first five months of this year, to implement (146) projects. The percentage of funding allocated to non-profit companies was 56%. In terms of the number of projects, 39 non-profit companies received funding amounting to 13.7 million dinars. The average amount of funding per project for non-profit companies reached 291,000 dinars.[34]

Article (12) of the legislation addresses the liquidation of the organization, stating that the Minister, upon the observer's recommendation, may instruct the organization to address the observer's notes regarding its activities within 30 days. Failing this, the Minister may refer the organization to the competent court for liquidation under certain conditions, including:

- violating the provisions of the law, this Regulation, or its articles of association;
- engaging in activities that do not align with its statutory goals;
- conducting activities that violate public order or moral standards.

Nevertheless, the shareholding corporate governance rules in Jordan are non-binding to the Limited Liability Companies, but they are binding to private shareholding and public shareholding whose subscribed capital exceeds 500,000 Jordanian dinars in accordance with the shareholding corporate governance for the year 2024 Issued pursuant to paragraph (a) of Article (151) of the Companies Law No. (22) of 1997 and its amendments.

Article (5/A and B) of the mentioned instructions stated that according to the duties of the board as outlined in the companies' law No. 22 of 1997 and its amendments and the company's bylaws, the board must develop internal regulations for the companies that govern financial, accounting, and administrative matters within the first four months of the fiscal year. These regulations should detail the board's duties, responsibilities, and relationship with senior executive management and required committees. Copies of these regulations must be provided to the department if requested by the Registrar and the regulations must approve policies and establish procedures, controls for internal auditing,

[34] Foreign Funding Unit, Report of Foreign Funding Provided to Associations and Non-Profit Companies and Cooperative Associations and Unions, 2024. https://www.mop.gov.jo/ebv4.0/root_storage/ar/eb_list_page/%D9%85%D9%84%D8%AE%D8%B5_%D8%AA%D9%82%D8%B1%D9%8A%D8%B1_%D8%A7%D9%84%D8%AA%D9%85%D9%88%D9%8A%D9%84_%D8%A7%D9%84%D8%A3%D8%AC%D9%86%D8%A8%D9%8A_%D9%84%D9%84%D9%81%D8%AA%D8%B1%D8%A9_%D9%83%D8%A7%D9%86%D9%88%D9%86_%D8%A7%D9%84%D8%AB%D8%A7%D9%86%D9%8A-%D8%A3%D9%8A%D8%A7%D8%B1_2024.pdf.

and risk management, including frameworks for handling transactions with related parties and measures to prevent conflicts of interest, ensuring compliance with environmental and societal responsibilities.

Article (6/a) of the said instructions states that the board must establish a permanent committee from its members or external experts, one of whom is an auditor, which according to article (7/a [1-4]) must carry out duties including review and periodically assess the accounting practices followed by the company and the financial manager's evaluations to ensure the effectiveness of financial management, review the financial statements, ensure their accuracy, and provide recommendations to the board for their approval. Additionally, offer recommendations on financial disclosures, ensure the continuity of the external auditor's engagement, review the auditor's report and observations regarding the financial statements, and address all matters related to the external auditor's work, including their observations, suggestions, and reservations, follow up on the company management's responses and present recommendations to the board, examine internal control systems, review and discuss internal audit plans, and assess their effectiveness.

7. Conclusion

Stemming from the Non-profit company's contribution in complementing the role of government in providing assistance to those in need globally as they enjoy public trust, they are the most targeted firms abused by terrorists aiming to finance terrorism interests.[35] According to the Companies Control Department website, the number of companies registered within its record until 28/08/2024 is (4161) varied between general partnership, limited partnership, limited liability and private shareholding.

As the number of such companies highly increases each year, the law should step in under certain circumstances to protect them from exploitation by terrorists to execute illicit activities. There are currently no formal regulations governing corporate governance in Jordan, except the Shareholding companies' governance instructions for the year 2024, which are binding only for the private shareholding companies, other companies shall be subjects to financial and legal control and

[35] FATF, Transparency and Beneficial Ownership. Paris, 2014. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-transparency-beneficial-ownership.pdf.coredownload.pdf.

compliance to governance rules. However, the Jordanian Companies Law does incorporate some principles of corporate governance within its articles.[36]

Although article (151) of company's law in force has been amended to oblige all public shareholding companies to comply with the governance principles, no other types of companies for such obligation were mentioned.

The instructions of shareholding corporate governance rules of 2024 are newly issued and still under experimental period and we can't figure out the results from applying such instructions to ensure the sufficient protection to the companies.

In my perspective, the absence of binding certain types of companies including, all companies with a capital of less than JOD 500,000 and the Non-Profit Companies in particular was one of the loopholes in the company act in force and such implementation requires amending the company law to include the obligatory implementation of good governance rules by the companies and ensuring compliance to these rules requires monitoring by a special unit with a mandate to effectively supervise, train, and do continuous assessment and adjustment.

The proposed law's provisions shall include all good governance rules, which can be achieved by appointing a Board of Directors with a high degree of understanding of the organization's goals and acting in their interest. The Board of Directors shall have the power to maintain and oversee the organization by establishing strong financial and human resources policies, meeting regularly, and monitoring activities closely.

Moreover, the Governance Principles shall be implemented by obliging all corporations regardless of type, structure, objectives, and capital to form committees including audit, risk management, remuneration, and corporate governance. Such committees shall have all rights to ensure the transparency and integrity of the company's business.

As formerly mentioned, to ensure the company's implementation of the good governance rules, it requires a special unit mandated by the law. The unit shall have two subsidiary divisions, one for supervising the works of the Non-Profit Companies to ensure their compliance with the company's law and good governance rules and the other division to prepare a training curriculum for corporate governance not only for the companies but also to the department's staff and evaluating their extent adoption of the measures and rules and preparing reports for advancement. Such amendments have to be included in both the

[36] Hetham Abu Karky – Hussien Suleiman AlHdaithat: Corporate Governance Approaches and Jordanian Companies Law. *Dirasat, Saharia and Law*, 1/2019.

company law which would be reflected in issuing a special regulation and also in the Company's Control Department structural chart.

The key players involved in initiating such amendment are the Cabinet, Minister of Industry, Trade and Supply, the General Control of Companies, and the Legislation and Opinion Bureau in Jordan. The reasoning for amending the company law is to serve the interests of Jordan, its economy, its financial system, to contribute to the safety and security of its citizens, and complete the implementation of measures approved by (FATF), to protect Jordan from a significant threat with potential adverse effects on foreign direct investment, international trade, and the inflow of foreign currency, to ensure the companies' compliance to company's law by existing a unit supervising their works, to help companies operate more efficiently, to improve access to capital, to mitigate risk and safeguard against mismanagement, to make companies more accountable and transparent to investors and give them the tools to respond to stakeholder concerns, to contribute to development by helping facilitate new investment, access to capital, and long term sustainability for firms, leading to economic growth and increased employment opportunities across markets.

The motivation behind proposing these changes is to penalize companies that don't comply with good governance regulations under Jordan's Penal Code. While some companies may argue that this will create extra burdens through increased scrutiny and sanctions, adhering to good governance actually enhances decision-making effectiveness, reporting accuracy, risk management awareness, and capital flow improvement. Additionally, it leads to a rise in the number of active firms, thereby bolstering sustainability efforts.

Bibliography

Éva Kuti: The Possible Role of the Non-Profit Sector in Hungary. *Voluntas: International Journal of Voluntary and Nonprofit Organizations*, 1/1990, 26–40. 26. http://www.jstor.org/stable/27927272. Accessed 18 July 2024.

Ismail Al Zyoud: The Role of Non-Governmental Organizations in Development of Jordanian Society. *Dirasat: Human and Social Sciences*, 1/2019.

RASHEED TI-JO, CSOs and NGOs. Ways of Financial Sustainability. Rasheed TI-JO Research Series: Third Sector. Vol.2. 2020.

FATF, IX Special Recommendations. Paris, 2001. . https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf.coredownload.pdf.

FATF, BPP-Combating the Terrorist Financing Abuse of Non-Profit Organisation. Paris, 2023.

Companies law and its amendments, 22, 1997. https://ccd.gov.jo/EBV4.0/Root_Storage/AR/r_Folder_/%D9%82%D8%A7%D9%86%D9%88%D9%86_%D8%A7%D9%84%D8%B4%D8%B1%D9%83%D8%A7%D8% AA_%D9%85%D8%B9%D8%AF%D9%84.pdf.

Jordan Economic Growth Plan 2018 – 2022-the economic policy council, Amman-Jordan.

Governance guidelines for non-profit companies, 2021.

The Register of Associations, the Companies Control Department, the Anti-Money Laundering and Counter-Terrorism Financing Unit. How to safeguard your organizations from the risks of terrorism funding, 2022.

Mohamed Jaffer – Syed Sohail: "Corporate governance issues in Family owned Enterprises." Published by CIPE, available on this site www.cipe.org(blog.p2.).

Cadbury Committee, 1992.

Bruno Dallago: Corporate Governance and Governance Paradigms. *Journal of Economics and Business*, 2/2002, 173–196. 174-175.

FATF, Combating the abuse of Non-Profit organizations (recommendation 8). Paris, 2015. https://www.fatf-gafi.org/media/fatf/documents/reports/BPP-combating-abuse-non-profit-organisations.pdf.

OECD, G20/OECD Principles of Corporate Governance 2023. OECD Publishing, Paris, 2023. https://doi.org/10.1787/ed750b30-en.

OECD, Risk management. In: *OECD Public Integrity Handbook*. OECD Publishing, Paris, 2020. https://doi.org/10.1787/ebbed075-en.

ABOU-EL-FOTOUH H. (N.D.), Importance Of Corporate Governance For SMEs, 2010.

Hetham Abu Karky – Hussien Suleiman AlHdaithat: Corporate Governance Approaches and Jordanian Companies Law. *Dirasat, Saharia and Law*, 1/2019.

FATF, Transparency and Beneficial Ownership. Paris, 2014. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-transparency-beneficial-ownership.pdf.coredownload.pdf.

SAFEGUARDING THE NON-PROFIT COMPANIES. THE ROLE OF THE RELATED SUPERVISORY AUTHORITIES TO MITIGATE THE RISKS OF TERRORIST FINANCING. CASE OF JORDAN-PAST AND PRESENT

Raghad Al-Shareedah[1]

ABSZTRAKT ■ Ez a cikk bemutatja a jogi személyek, köztük a Nonprofit Társaságok helytelen használatának problémáját, amelyek a Nonprofit Szervezetek FATF-meghatározása alá tartoznak. Az ilyen társaságok létfontosságú szerepet játszanak különböző nemzetgazdaságokban, társadalmi intézményekben és a globális gazdaságban. A nonprofit szervezetek kezdeményezései támogatják a vállalati és kormányzati szektor munkáját azáltal, hogy világszerte létfontosságú szolgáltatásokat, vigaszt és reményt nyújtanak a rászoruló embereknek. A terroristák és terrorista csoportok kihasználják a nonprofit szerepeket, hogy pénzt szerezzenek és osszanak szét, logisztikai támogatást nyújtsanak, előmozdítsák a terroristák toborzását, és más módon támogassák a terrorista csoportokat és tevékenységeiket.
A cikk bemutatja Jordánia útját e probléma kezelésében, valamint a felügyeleti hatóságok jelentős szerepét, amelyek felhatalmazással rendelkeznek az ilyen szervezetek pénzügyi és jogi nyilvántartására, ellenőrzésére és szabályozására; valamint azt, hogy ezek a hatóságok hogyan járultak hozzá ahhoz, hogy a hatályos jogszabályok módosításával és az alkalmazott intézkedések terén tett jelentős erőfeszítésekkel Jordánia lekerüljön a FATF szürkelistájáról.

ABSTRACT ■ This article will demonstrate the issue of misusing legal persons including the Non-Profit Companies which fall under the Non-Profit Organizations FATF definition. Such Companies play a vital role in various national economies, social institutions, and the global economy. The Non-Profit organizations' initiatives support the work of the corporate and governmental sectors in offering vital services, consolation and hope to individuals in need globally. The terrorists and terrorist groups take advantage of the nonprofit roles to acquire and distribute money, offer logistical support, promote the recruitment of terrorists, and support terrorist groups and activities in other ways.
It will present Jordan's journey in tackling this issue and the significant role played by the supervisory authorities having the mandate to register, monitor and control them financially and legally and how they contributed in removing Jordan from the FATF grey list upon amending the legislation in place and exerting significant efforts in the measures implemented.

[1] PhD Student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

1. Introduction

Given Jordan's advantageous geographical location and central role in the Middle East's peace process, there have been increased risks associated with terrorism and its financing. This includes the emergence of terrorist groups, networks, and cells that contribute to regional terrorism, both intellectually and organizationally, particularly following the Iraq war.

Jordan, along with its citizens, officials, and institutions, has been a longstanding target for terrorist activities due to its proactive stance against all forms of terrorism. Despite enduring the consequences of terrorism, Jordan consistently emphasizes the need for international collaboration in confronting and eliminating terrorism by establishing mechanisms to counteract its funding, training, and practice.[2]

Moreover, Jordan as a member of the Middle East & North Africa Financial Action Task Force (MENAFATF) has been a key partner in regional and international efforts to combat terrorism and counter anti-money laundering and has to comply with FATF recommendations and reflecting them to the relevant legislation.

As stated in the Interpretive Note accompanying Recommendation 8, terrorist groups utilized a number of methods including Non-Profit companies (NPC) for purposes such as fundraising, facilitating the movement of funds, providing logistical assistance, recruiting individuals for terrorist activities, or otherwise supporting terrorist organizations and their operations. They may exist in various structures, such as a sole proprietorship (including personal charitable donations), an unincorporated association, a corporation, a foundation (characterized by its funding from a founder and organized as a trusteeship), or a condominium. Consequently, safeguarding the NPC sector from terrorist exploitation is not only vital in the global effort against terrorism but also essential for maintaining the integrity of such sector and ensuring the trust of donors.

Corporations fulfill a crucial and lawful function in the economy of any jurisdiction, serving as valuable instruments for commercial and entrepreneurial endeavors. Nevertheless, these inherent traits render them, under specific circumstances, appealing to criminals who might intend to exploit them as instruments for unlawful activities.

The registration of these companies falls under the supervision of the Companies Control Department (CCD) collaborating with the Anti-Money Laundering and Countering Financing Terrorism Unit and other related entities in case of noncompliance and infringements. Such companies may be manipulated for terrorist financing purposes, channeling legitimately acquired funds to support terrorist activities or groups.[3]

The general meeting of the FATF in February 2010 decided that the anti-money laundering and terrorist financing system in Jordan needs to be reviewed under international recommendations in this regard, given that the Kingdom obtained a degree of

[2] "مكافحة الإرهاب والتطرف العنيف." وزارة الخارجية وشؤون المغتربين, Jan. 2024, mfa.gov.jo/content/%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%A7%D9%84%D8%A5%D8%B1%D9%87%D8%A7%D8%A8-%D9%88%D8%A7%D9%84%D8%AA%D8%B7%D8%B1%D9%81-%D8%A7%D9%84%D8%B9%D9%86%D9%8A%D9%81.

[3] FATF, Money Laundering and Terrorist Financing Risk Assessment of Legal Persons and Legal Arrangements in Jordan. Paris, 2023.

(noncompliant) and (partially compliant) in (14) recommendations out of (16) basic and major international recommendations according to the results of the Kingdom's joint evaluation report approved by the Financial Action Task Force for the Middle East and North Africa region in May 2009.[4]

Thus, Jordan as a member of the Middle East & North Africa Financial Action Task Force (MENAFATF) which is the member of FATF passed through a review to its process by the review team initiated at the level of Africa and the Middle East appointed by the International Cooperation Review Team.

The mutual evaluation report for Jordan in 2019 highlighted significant shortcomings in its Counter-Terrorist Financing system, indicating a low level of effectiveness relating to transparency of beneficial ownership information (Immediate Outcome 5), risks associated with the potential abuse of non-profit organizations for terrorist financing (Immediate Outcome 10), noncompliant to recommendation (8) governing the issue of non-profit organization and compliant to recommendation (6) about the targeted financial sanctions related to terrorism & terrorist financing.[5]

As a result, to these findings, Jordan was placed in the grey list in October 2021 and committed to executing an action plan and measures to address these issues.

Jordan exerted extensive efforts since receiving its first mutual evaluation report by FATF in 2009, which analyzes the level of Jordan's compliance with the FATF (40) Recommendations and the level of effectiveness of its countering financing of terrorism system and provides recommendations on how the system could be strengthened.

On the one hand, this document explores the deficiencies and shortcomings labeling Jordan as a noncompliant jurisdiction to specified recommendations, which resulted in categorizing it in the grey list by FATF in October, 2021 as such inclusion indicates that the country is moving towards the black list, posing a significant threat with potential adverse effects on foreign direct investment, international trade, and the inflow of foreign currency.

On the other hand, it presents the strategies and action plans implemented by the supervisory authorities in Jordan to provide protection to the legal persons including the non-profit companies from being misused for the purposes of funding terrorism encompassing legal and technical reforms in this regard.

2. Chronological Order of Jordan's History Place According to FATF Assessment to Counter the Funding of Terrorism

Jordan always stresses the importance of responding to the threat of terrorism in a comprehensive manner that ensures peace and security, supports political solutions and development programs and addresses the sources that fuel terrorism and violence.

Jordan was among the countries to be assessed due to the absence of measures tackling the deficiencies in the implemented strategies and underwent an assessment by MENAFATF, adhering to the 40 recommendations established by the FATF in 2012, along with any subsequent amendments, and utilizing the methodology adopted in

[4] FATF, The Hashemite Kingdom of Jordan's MER. Paris, 2019. https://www.menafatf.org/information-center/menafatf-publications/hashemitekingdom-jordan-mutual-evaluation-report.

[5] Ibid.

2013, also considering subsequent amendments and the nine special recommendations on terrorism financing from 2001. The evaluation was conducted using the anti-money laundering and countering the financing of terrorism methodology from 2004[6].

In 2008, the evaluation team paid an on-site visit to do their assessment based on information gathered from the competent authorities, including the Central Bank of Jordan, Ministry of Justice, Ministry of Interior, Ministry of Finance, the Anti-Money Laundering and Counter Terrorist Financing Unit and Companies Control Department. Such information includes the legislation, regulations, and additional documentation in place.

The first mutual evaluation report of Jordan adopted by MENAFATF in 2009 issued the evaluation made by the said team, in which they assessed Jordan's adherence to the FATF 40+9 recommendations and offered suggestions for enhancing specific aspects of the system. Accordingly, the mentioned authorities worked extensively to address the strategic highlighted deficiencies.

FATF members during the February 2010 Plenary agreed that Jordan should undergo a comprehensive reassessment regarding its adherence to international combating the financing of terrorism (CFT) standards. This decision stemmed from the results of the mutual evaluation of Jordan, where Jordan was evaluated as (noncompliant) and (partially compliant) in (14) out of (16) core and key recommendations.[7]

The first review process with Jordan was initiated in 2010 when the International Cooperation Review Group (ICRG), designated such task to the Regional Review Group of Africa and the Middle East (RRG). This happened when Jordan substantially addressed the strategic deficiencies identified in the FATF's targeted review. FATF decided that it will no longer monitor Jordan through the ICRG monitoring process.

In June 2021, Jordan amended its counter-terrorism legislation directly in response to its 2019 Mutual Evaluation Report (MER). Regrettably, the changes came into effect after the FATF's deadline, which contributed to the country being placed on the grey list in October 2021. This list comprises countries collaborating with the FATF to rectify strategic shortcomings in their systems for combating money laundering, terrorist financing, and proliferation financing.

Jordan acknowledged its achievements in enhancing the domestic framework to counter-terrorist financing with the main focus on the protection of non-profit organizations and companies that fall under the FATF definition, aligning it with global standards, and successfully fulfilling all the components of the action plan endorsed by the Financial Action Group (FATF) for Jordan in October 2021.

In October, 2023, Jordan as a response to FATF recommendations intensified its efforts to mitigate the risks of terrorist financing and was among countries to be taken off from the FATF Grey List. Getting off the said list highlighted the significance of consistently updating the Jordanian system to prevent from reverting to the list and to uphold its global reputation in the fight against the financing of terrorism.

[6] Middle East & North Africa Financial Action Task Force, Mutual Evaluation Report of the Hashemite Kingdom of Jordan. MENAFATF, 2009. https://www.menafatf.org/sites/default/files/MER_Hashemite_Kingdom_of_Jordan.pdf.

[7] https://www.amlu.gov.jo/EN/Pages/Regime_process_Review.

3. FATF Recommendations to be adopted by the Supervisory Authorities to Tackle the Issue of Misusing the Non-Profit Companies for the Purposes of Funding Terrorism

The following measures shall be implemented by Jordanian Supervisory Authorities. Such Measures were set out in the unique FATF recommendation (8) to combat terrorist financing along with other measures as outlined in the noteworthy recommendations including (1, 5, 6, and 24) that contributed in the fight against the financing of terrorists.

3.1. Recommendation (8): Measures to Prevent the Misuse of Non-Profit Organizations

Recommendation (8) set out by FATF states the following:
"Countries should review the adequacy of laws and regulations that relate to non-profit organisations which the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused and proportionate measures, in line with the risk based approach, to such non-profit organizations to protect them from terrorist financing abuse, including: (a) by terrorist organizations posing as legitimate entities; (b) by exploiting legitimate entities as conduits for terrorist financing including to escape asset-freezing measures; and (c) by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organizations."[8]

FATF's concentration on the Non-Profit Organizations (NPOs) sector lies on several reasons as they might frequently operate with minimal or zero governmental supervision, such as in the aspects of registration, record-keeping, reporting and monitoring. The creation of NPOs may involve few formalities, such as lacking prerequisites for skills or starting capital, and may not mandate background checks for employees. Exploiting these characteristics, terrorist organizations have capitalized on the vulnerability of NPOs, infiltrating the sector and misusing their funds and operations to camouflage or facilitate terrorist activities.[9]

For the implementation of this recommendation, FATF adopted a definition applied to the legal entities or arrangements primarily involved in raising or disbursing funds for charitable, religious, cultural, educational, social, fraternal purposes, or other forms of "good works" (referred to as the "FATF definition").[10]

Such a definition does not encompass the entire spectrum of not-for-profit entities. They vary in their susceptibility to terrorism financing abuse based on their types, activities, or characteristics, with the majority likely to present a low risk.

[8] FATF, Combating the abuse of Non-Profit organizations (recommendation 8). Paris, 2015. https://www.fatf-gafi.org/media/fatf/documents/reports/BPP-combating-abuse-non-profit-organisations.pdf.

[9] FATF, IX Special Recommendations. Paris, 2001. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf.coredownload.pdf.

[10] FATF, BPP-Combating the Terrorist Financing Abuse of Non-Profit Organisation. Paris, 2023. www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Bpp-combating-abuse-npo.html.

3.2. Recommendation (1) and its Interpretative Note: Assessing Risks and Applying a Risk-Based Approach

All Jurisdictions must recognize, evaluate, and comprehend the risks associated with money laundering and terrorist financing within their borders. They should then implement measures, such as appointing an authority or system to coordinate efforts in risk assessment and allocate resources appropriately to effectively mitigate these risks.

3.3. Recommendation (5) and its Interpretive Note: The Criminalization of Terrorist Financing

This recommendation comes to ensure that all states including Jordan shall possess the legal framework necessary to prosecute and impose criminal penalties on individuals and legal persons who finance terrorism. Therefore, it mandates countries to designate terrorist financing offenses as predicate offenses.

The interpretive note (5) states that legal entities should face criminal liability and sanctions, and in cases where this is not feasible due to fundamental principles of domestic law, civil or administrative liability and sanctions should be imposed. This should not hinder simultaneous criminal, civil, or administrative proceedings against legal entities in jurisdictions where multiple forms of liability are applicable. These actions should not exempt natural persons from criminal liability. All sanctions must be effective, proportionate, and serve as a deterrent.[11]

The basis of the adherence to this recommendation and its interpretive is the provisions contained in article (5) of the United Nations Convention for the Suppression of the Financing of Terrorism 1999, which Jordan ratified under the Law of Ratification of the International Convention for the Suppression of the Financing of Terrorism of 2003.

3.4. Recommendation (6): Financial Sanctions Related to Terrorism & Terrorist Financing

Each country is mandated to implement targeted financial sanctions to adhere to the United Nations Security Council Resolutions. With regard to Jordan, sentences for natural and legal persons who commit terrorist financing acts are non-dissuasive, disproportionate under the terrorism prevention law of 2006. It is not possible to measure the effectiveness due to the absence of evidence and the absence of statistics.

Concerning legal entities, Jordan's Penal Code specifies that judgments against them can only involve fines and confiscation. The absence of any mention of a fine or confiscation penalty in article (7) of the Terrorism Prevention Law (TPL) is attributed to the provisions of article (74) of the Penal Code. According to paragraph (3) of Article (74) and if the law prescribes a primary penalty other than a fine, that specified penalty would be replaced by the fine, and legal entities would be subject to a fine within the

[11] FATF, Guidance on the criminalisation of terrorist financing (Recommendation 5). Paris, 2016. www.fatf-gafi.org/publications/fatfrecommendations/documents/criminalising-terrorist-financing.html.

limits outlined in articles (22 to 24). Consequently, the penalty imposed on legal entities cannot be deemed dissuasive or proportionate.

Additionally, in line with article (74), there is the possibility of implementing further precautionary measures, such as suspension or dissolution of a legal entity, as outlined in articles (36) and (37) of the Penal Law.

3.5. Recommendation (24): Beneficial Ownership of Legal Persons

In March 2022, FATF implemented vigorous global regulations regarding beneficial ownership, aimed at thwarting criminals' efforts to conceal illicit activities through opaque corporate structures. These regulations are designed to ensure that relevant authorities have access to comprehensive, accurate, and up-to-date information regarding the actual owners of companies. They mandate that beneficial ownership details be maintained by a public entity serving as a beneficial ownership registry or an alternate system facilitating efficient information retrieval.[12]

Furthermore, the guidance outlines various types and sources of pertinent information, as well as mechanisms for obtaining such data. One notable aspect is the adoption of a multi-faceted approach, which involves gathering information from diverse sources, such as the companies themselves, public registries, or alternative mechanisms ensuring swift access to beneficial ownership information. FATF's mutual evaluations have demonstrated that jurisdictions employing this multifaceted approach are more successful in preventing the misuse of legal entities for criminal purposes and enhancing transparency regarding beneficial ownership, compared to those relying on a singular method.[13]

These measures are intended to address regulatory gaps and weaknesses that have allowed fraudulent entities to operate as fronts for criminal endeavors or to evade tax obligations for an extended period. They aim to streamline the process for investigators to ascertain the genuine beneficial owners of companies swiftly and efficiently. Ultimately, these changes are geared towards combating financial crimes, reducing corruption and tax evasion, and fostering sustainable economic development.[14]

4. The Role of the Relevant National Supervisory Authorities in Jordan: Companies Control Department and the Anti-Money Laundering and Counter the Financing of Terrorism Unit-Past and Present

4.1. FATF's Identified Deficiencies: The Non-Profit Organizations Sector

The nine special recommendations issued by FATF acknowledging the crucial need to take proactive measures in countering the funding of terrorism including the protection of non-profit organizations from being misused by terrorists to facilitate the movement of funds for supporting terrorism activities. Following these recommendations, the best

12 FATF, Guidance on Beneficial Ownership for Legal Persons. Paris, 2023. http://www.fatf-gafi.org/publications/FATFrecommendations/guidance-beneficial-ownership-legalpersons.html.

13 Ibid.

14 Ibid.

practices paper (BPP) on combating the abuse of non-profit organizations by (FATF) was initially drafted in 2002 in which they introduced standards aimed at addressing specific vulnerabilities and threats related to terrorist financing (TF).[15]

In June 2014, FATF released a typology report on the risk of terrorist exploitation to non-profit companies, prompting further amendments to the BPP in 2015. These revisions integrated the findings from the typologies report and the incorporated additional insights and examples of best practices from governments, Non-Profit Companies (NPC)s, and financial institutions.[16]

In June 2016, after engaging extensively with the NPC sector and witnessing instances of the overly broad application and misapplication of recommendation (8), FATF made revisions to both recommendation (8) and its accompanying interpretive note.[17]

Accordingly, Jordan did not fulfill several crucial obligations essential for a comprehensive combating system[18] and was under increased monitoring as being noncompliant. As a result, FATF paid an on-site visit to the supervisory authorities including Companies Control Department, the Anti-Money Laundering Unit and other related entities to make an analysis of the legal and regulatory framework, institutional framework, preventive measures pertaining to the recommendation eight. FATF's evaluation based on the regulations in place was made available by the mentioned laws, e.g. the anti-money laundering law, the terrorism prevention law, the Jordanian penal code, the law on penal courts, the law on anti-corruption authority, the companies' law, the exempted companies' regulation, etc.

The legislations in place were not updated to keep pace with evolving threats and techniques used by individuals and entities engaged in terrorist financing. Outdated laws may lack provisions to address emerging risks effectively. So, the legal framework in Jordan lacks primary or delegated legislations that mandate compliance with the fundamental requirements specified in certain FATF recommendations.

Regarding the criminalization of terrorist financing, Jordanian lawmakers established the legal framework for this act by including the terrorist financing crime under the terrorism prevention law issued in November 2006 and considering terrorist financing a terrorist act. The criminalization scope mentioned in the terrorism prevention law does not extend to include acts committed by terrorist organizations or terrorists to be in conformity with the International Convention for the Suppression of the Financing of Terrorism. It is noticeable that the concept of funds is not clear in relation to terrorist financing in the said law. Sentences for natural and legal persons who commit terrorist financing acts are non-dissuasive, disproportionate. It is not possible to measure the effectiveness due to the absence of evidence and the absence of statistics.

15 FATF 2015.

16 FATF 2023.

17 CGCC, To protect and prevent outcomes of a global dialogue to counter terrorist abuse of the nonprofit sector, 2013. https://www.globalcenter.org/wp-content/uploads/CGCC_Prevent-Protect-Report_pgs.pdf.

18 Middle East & North Africa Financial Action Task Force, Mutual Evaluation Report of the Hashemite Kingdom of Jordan. MENAFATF, 2009. https://www.menafatf.org/sites/default/files/MER_Hashemite_Kingdom_of_Jordan.pdf.

Concerning legal entities, the Penal Code specifies that judgments against them can only involve fines and confiscation. The absence of any mentioning of a fine or confiscation penalty in Article (7) of the Terrorism Prevention Law (TPL) is attributed to the provisions of Article (74) of the Penal Code. According to paragraph (3) of Article (74), "(...) and if the law prescribes a primary penalty other than a fine, that specified penalty would be replaced by the fine, and legal entities would be subject to a fine within the limits outlined in Articles 22 to 24." Consequently, the penalty imposed on legal entities cannot be deemed dissuasive or proportionate.[19]

Additionally, in line with Article (74), there is the possibility of implementing further precautionary measures, such as prohibiting a legal authority from operating or dissolving it, as outlined in Articles (36 and 37) of the Penal Law.[20]

Jordan's company law did not statute any articles regarding the legal persons in case of exercising a direct or indirect illicit activities for the purposes of financing terrorism through their management or mentioning of any penalties sentenced. Moreover, the declaration by the partner/shareholder to determine the real beneficiary when registering companies, which must be submitted, is not included in the said law. The absence of such measures will contribute to the increase of misusing non-profit organizations and all registered companies in Jordan.

Another system shortcoming is the absence of a risk-based approach for Non-Profit Companies registered in favor of the Companies Control Department, as such an approach would protect this particular sector from being misused to fund terrorism.

The Department shall cooperate to specify and define the vulnerabilities and threats exposing such companies to risks, which an estimated (1589) companies fall within its supervisory and are exposed to high, medium, and low risks.

With respect to national collaboration, there is no indication of a clear policy or any established mechanism for cooperation and coordination among the relevant authorities concerning combating the financing of terrorism.

As for international collaboration, Jordan has ratified the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna) and the UN Convention for the Suppression of the Financing of Terrorism. However, it is important to note that these conventions have not been fully implemented.

There are no existing laws or measures ensuring a prompt and effective response to mutual legal assistance requests from foreign countries, particularly when such requests pertain to properties of equivalent value. Furthermore, there are no specific arrangements to coordinating seizure and confiscation measures with other countries. In terms of extradition, Jordan cooperates extensively, overcoming legal or practical obstacles to provide assistance in cases where both countries criminalize the primary act of the crime.

Law enforcement agencies and the relevant supervisory authorities face a shortage of resources including inadequate funding, staffing and technological resources can hamper the ability of supervisory authorities to carry out effective monitoring, inspe-

[19] Ibid.
[20] Ibid.

ctions and investigations. Furthermore, employees within these competent authorities lack adequate training related to AML/CFT.[21]

Jordan must enhance both human and technical resources across various competent authorities crucial to the effectiveness of the combating system. The number of human resources in each authority does not exceed approximately (200) and those who worked on the issue of exercising legal and financial supervisory are between (15-20) employees due to extensive in-house work.

The deficiency in these resources currently hampers the efficiency of the system. Moreover, there is insufficient awareness for budgeted reasons among both the officials and private sectors regarding terrorist financing risks, both in terms of their vulnerability to exploitation for illicit transactions and the potential consequences.[22]

In conclusion, the main areas of strategic deficiencies identified by FATF to be addressed by the supervisory authorities are for example the lack of sufficient laws and regulations related to combating the funding of terrorism, lack of satisfactory and adequate regulatory and supervisory frameworks, lack of robust and effective measures including lack of transparency in beneficial ownership information, lack of international cooperation, limited risk assessment, lack of collaboration with the private sector, human resources and technological challenges.

Thus, Jordan was required to do legislative reforms and enhance the role of the supervisory authorities in countering all means utilized by the terrorists to legalize their illicit activities and to establish targeted financial sanctions regimes in line with United Nations Security Council resolutions aimed at preventing and suppressing terrorism and terrorist financing.

4.2. Jordan's Reforms and Compliance to FATF Recommendations

Jordan is at the forefront of countries fighting terrorism and extremism within a comprehensive approach based on legislative, intellectual, security and military dimensions.

Jordan's position on the phenomenon of terrorism and extremism stems primarily from the message and legitimacy of the Hashemite leadership and from the cultural composition of the Jordanian people, which respects moderation and rejects extremism and the use of religion and ideologies to spread violence, hatred, and incite terrorism.[23]

Jordan is working with the international community to formulate a comprehensive approach to dealing with the threat of terrorism, which is no longer just a challenge facing a specific country, region or component, but rather a target that reaches the level of a threat and affects the entire international community.[24]

To align with FATF standards in the designated domains and perform the required reforms, Jordan has been actively addressing the deficiencies identified in the Mutual

[21] Ibid.
[22] Ibid.
[23] https://www.mfa.gov.jo/content/%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%A7%D9%84%D8%A5%D8%B1%D9%87%D8%A7%D8%A8-%D9%88%D8%A7%D9%84%D8%AA%D8%B7%D8%B1%D9%81-%D8%A7%D9%84%D8%B9%D9%86%D9%8A%D9%81
[24] Ibid.

Evaluation Report (MER), particularly in the recommendations where the country requested re-rating. These recommendations include (1, 5, 6, 8, 24) and stress the necessity of complying with and fully implementing Security Council Resolutions related to combating terrorism, the most important of which are resolutions No. (1267, 1989, 2253, 1373 and other relevant resolutions) aimed at drying up the sources of terrorism.[25]

As per for FATF recommendations and their interpretive notes, Jordan ought to assess the effectiveness of their laws and regulations concerning entities susceptible to exploitation for terrorism financing. Non-profit organizations, in particular, face heightened vulnerability, and the authorities are advised to take the following actions:[26]

1. Broaden the scope of Terrorism Financing (TF) criminalization to encompass actions potentially undertaken by terrorist organizations or individuals involved in terrorism, aligning with the UN Convention for the Suppression of the Financing of Terrorism.
2. Provide a clear definition for the concept of funds under the UN Convention for the Suppression of the Financing of Terrorism.
3. Establish a penalty that is both dissuasive and proportionate for individuals and legal entities found guilty of committing the TF crime.
4. Addressing these challenges requires a comprehensive and coordinated effort involving legislative updates, enhanced enforcement powers, sufficient resources, international collaboration and ongoing risk assessments. Regular reviews and adjustments to legislation and regulatory frameworks are crucial to adapt to emerging threats and close loopholes effectively. Additionally, supervisory authorities should work closely with relevant stakeholders, including the private sector and international partners, to strengthen the overall effectiveness of anti-terrorist financing measures.
5. Authorities responsible for setting up, registering, and granting licenses to legal entities are required to acquire precise and current details regarding the individuals who ultimately benefit from these entities.
6. The relevant entities must identify, evaluate, comprehend and oversee the risks associated with money laundering and terrorist financing. This process should consider risk factors associated with customers, countries, geographical regions, products, services, channels, transactions, and evolving techniques. The assessment should be appropriate to the nature and scale of the reporting entity, comply with supervisory authority requirements, and align with the national risk level.

For the purposes of setting-up the plans necessary for the implementation of the abovementioned tasks and developing the general policy for anti-money laundering and counter terrorist financing, the National Anti-Money Laundering and Counter Terrorist Financing Committee was reconstituted per the provisions of Article (5) of the Anti-Money Laundering and Terrorist Financing Law No. 20 of 2021 and is comp-

[25] Ibid.

[26] FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Paris, 2012-2023. www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

rised of higher level of officials representing the governmental ministries, enforcement, supervisory, regulatory and related authorities.[27]

Although recommendation (8) is concerned with Non-Profit Companies as being a tunnel for terrorists to exercise their illegal aims, it does not function independently. Its implementation should align with the broader principles outlined in recommendation (1), which emphasizes the adoption of a risk-based approach, recommendation (24) concerning the importance of beneficial ownership to reduce the misuse of legal entities if information regarding the legal owner and the beneficial owner, the source of the corporate vehicle's assets and its activities becomes available to the authorities in a timely manner, recommendation (5) criminalizing the funding of terrorism, recommendation (6) targeted at the financial sanctions related to terrorism & terrorist financing. Accordingly, two working teams have been established, each representing relevant national authorities. One team focuses on establishing a beneficial ownership registry, while the other is tasked with devising a methodology to conduct risk assessments pertaining to legal entities and arrangements.

The adoption of FATF recommendations is not only restricted to the said committees, the Companies Control Department and the Anti-Money Laundering and Countering Terrorist Financing Unit also play an important role mandated by their respective laws in ensuring the implementation of a number of principles to advance Jordan's rank in terms of combating financing terrorism.

The former has a mandate to register, monitor, control companies' businesses and the latter receives reports regarding transactions possibly linked to money laundering or financing terrorism, requesting relevant information, scrutinizing and probing these transactions. It is responsible for preparing a report attached to information, data and documents related to the existence of a transaction suspected of being linked to terrorist financing and refers it to the competent public prosecutor to conduct an investigation into it.[28]

4.2.1. The Companies' Control Department

The Companies' Control Department (CCD), operates under the Ministry of Industry, Trade and Supply of Jordan and is responsible for registering various types of companies, including the Non-Profit Companies are registered in a special record.

The department plays a crucial role in ensuring the proper functioning, transparency, and compliance of companies to the company law No. (22) of 1997 and its amendments, which is the governing law to oversee the businesses of Jordanian companies legally and financially.

To implement recommendation (8), FATF defines a non-profit organization as a legal entity, arrangement, or organization primarily involved in collecting or distributing funds for charitable, religious, cultural, educational, social, purposes, or for other altruistic endeavors.[29] All member states to FATF shall specify that all companies fall under the definition of FATF and use all related information to identify the types and

[27] https://www.amlu.gov.jo/Default/Ar.
[28] Ibid.
[29] FATF 2023.

characteristics that may expose non-profit companies to abuse due to the nature of businesses, the nature of threats and how terrorists' abuse of non-profit companies shall be defined.

FATF's definition applies to the NPCs that fall under the supervision of the department. Only companies carrying out businesses in the health sector, education sector, microfinance, investment promotion and training or any other objective in the form of a limited liability, private shareholding, general partnership or limited partnership company are registered in the records of CCD. As stated in the interpretive note accompanying recommendation (8), terrorists and terrorist groups may utilize certain NPCs within the sector for purposes such as fundraising, facilitating the movement of funds, providing logistical assistance, recruiting individuals for terrorist activities, or otherwise supporting terrorist organizations and their operations. This exploitation not only enables terrorist actions but also undermines donor trust and jeopardizes the fundamental integrity of NPCs. Consequently, safeguarding the NPC sector from terrorist exploitation is not only vital in the global effort against terrorism, but also essential for maintaining the integrity of the NPC sector and ensuring the trust of donors. The number of registered Non-Profit Companies till this date reached (1589) according to the website of the Companies' Control Department.

Recommendation (8) is designed to specifically target NPOs that present the highest risk of being exploited for terrorist financing activities. The aim of the recommendation is to prevent such companies from being exploited by terrorist groups as they may be susceptible to exploitation by terrorists for various reasons as they benefit from public trust, possess access to significant funding sources and frequently deal with cash transactions. Moreover, some NPOs operate globally, facilitating both national and international operations and financial transactions, often in regions prone to terrorist activities. where companies experienced minimal government oversight, such as in registration, record-keeping, reporting, and monitoring. Alternatively, the creation of NPOs may require few formalities, with no mandatory qualifications or starting capital and background checks for employees might not be obligatory. Terrorist groups have exploited these characteristics of NPOs to infiltrate the sector, misusing NPO funds and operations to conceal or support their terrorist activities.

Jordan's legislations in place as the Jordanian Non-Profit Companies Regulation No. 73 of 2010 and its amendments stipulates in article (9) that the company during the first three months of the beginning of the fiscal year shall provide an annual report containing its operations, activities and sources of funding, accompanied by its balance sheet certified by the company's authorized signatories, its auditor, any other information that the Controller may request, the business plan, its activities, the projects expected to be implemented during the year and a detailed statement of financing for these activities and projects. This ensures that they are complying with the law and the CCD staff can do their work by investigating their businesses clarified by the auditor.

The legislation in place pertaining to the compliance of the non-profit companies to the effective law remains ineffective to ensure that they are not abused for the purposes of financing terrorism. To adhere to FATF recommendations the Companies' Control

Department worked on modifying the company law and amended the article (273) and added article (273/bis) to the said law including the following:

1. The registered companies shall disclose all information regarding the real beneficiary of shares in the company. All companies shall maintain a record that includes information about the real beneficiary and any changes that occur to his data, within a certain period of the change occurring or registering the change with the department and the controller has the right to request any document or information that allows him to check the accuracy of the information provided about the company.
2. Companies must correct their status within a maximum period of three months from the effective date of the provisions of the amended law, so that their basic data and information are amended in accordance with the instructions issued for this purpose.
3. The General Controller of Companies is required to record the name of the real beneficiary in an electronic register containing data and information, so that all or any part of it is available to the public or linked to the databases of the relevant authorities.
4. The controller should cooperate with international counterparts and follow up on the quality of assistance provided in response to requests for international cooperation regarding basic information of registered companies, information of beneficial owners, and determining the whereabouts of those residing abroad in accordance with applicable legislation or in accordance with the principle of reciprocity, as the provisions of this article are implemented under a system issued for this purpose.
5. The company in case of a breach of law shall be penalized with a fine between 2,000-20,000 Jordanian dinars or imprisonment for a period not exceeding one year, or both penalties.
6. The Companies' Control Department issued the beneficial ownership registry regulation No. 26 of 2022 to implement the provisions mentioned in article (273, paragraph D) as mentioned above.

The above-mentioned amended company law No. 19 of 2021 was issued on September 16, 2021 by adding Article (273/bis) in order to be consistent with the legislation issued by the Central Bank of Jordan. Its significance lies in not only safeguarding non-profit companies from being exploited for the purposes of financing terrorism but also all registered companies in Jordan and meeting the requirements of the relevant objectives of the Anti-Money Laundering and Countering the Financing of Terrorism Law.

The amended companies law No. 20 of 2023 that was issued on August 13, 2023, is as another achievement for Jordan and specifically for the Companies' Control Department. The amendments contribute to achieving stability and ensuring the effectiveness of the measures taken by the department to improve the Kingdom's classification in combating money laundering and terrorist financing according to (FATF). Article (285) was amended in the mentioned law by giving the Controller of Companies the power to notice the company by announcing on the department's official website that it was

listed among suspended companies after one month from the date of the notice in cases i) if a company fails to adjust its situation in accordance with the provisions of the law, ii) if it did not prove that it no longer has headquarters, iii) if it ceased to carry out its business or the duties imposed on it by law, iv) if a period exceeding (6) months has passed without election of the general manager of the company or a board of directors. In this case, the company is prohibited from carrying out any actions and its manager or board of directors also loses all their power. The article also states that when the Controller checks the status of the company, he has the power to proceed with the required procedures to dissolve the company in case the company remains listed among suspended companies for more than a year without executing the necessary actions and procedures to move to the operating companies' registry upon the request of the company. The suspension or dissolution of a legal entity is considered as implementation of precautionary measures in line with what is outlined in articles (36) and (37) of the Penal Law and in line with article (74) of the same law.

The adoption of a risk-based approach is also required by FTAF recommendation (1). It acts as a guiding principle for countries, directing their resources and focusing efforts on addressing identified high-risk deficiencies in their systems.

Adopting a "one size fits all" strategy would contradict recommendation (1) and hinder the effective implementation of a risk-based approach. Simultaneously, Jordan may employ measures tailored to the risks identified in its domestic assessment of the NPO sector and its comprehension of the Terrorism Financing (TF) risks specific to the sector.

For the purposes of conducting the said approach, a team was formed in 2022 to define the threats and vulnerabilities of exposing to risks of misuse to fund terrorists to all legal persons. While the approach targeting non-profit companies was prepared in 2022 by a committee formed to classify non-profit organizations to certain characteristics resulting from intensive investigation to the sector concluded with the low level of vulnerability threats that companies have to face.

The non-profit companies identified with exposing themselves to vulnerable financing terrorism threats are (23) with medium and low risks.

4.2.2. The Anti Money-Laundering and Counter Financing Terrorism Unit

The Anti-Money Laundering and Counter Financing Terrorism Unit was established in Jordan in accordance with the Anti Money Laundering and Counter Terrorist Financing Law No. 46 of 2007.[30]

The primary duties of the Unit include receiving notifications concerning transactions that are suspected to be involved with money laundering or terrorist financing. The unit has the right to exchange information with counterpart units on the condition of reciprocity and that this information is only used for purposes related to combating money laundering and the financing of terrorism and on the condition of obtaining the approval of the counterpart unit that provided that information.[31]

[30] https://www.amlu.gov.jo/.

[31] https://www.amlu.gov.jo/Ar/Pages/%D9%86%D8%A8%D8%B0%D8%A9_%D8%B9%D9%86_%D8%A7%D9%84%D9%88%D8%AD%D8%AF%D8%A9.

According to FATF recommendations resulting from the outcome of the Kingdom's mutual assessment process, the Unit implemented effective strategies that are compatible with international standards. These efforts included reviewing its legislations result in amending the Anti-Money Laundering and Counter Terrorist Financing Law No. 46 in 2007, which underwent a significant transformation with the enactment of Law No. 20 of 2021.

The provisions of the new amended Law of Anti-Money Laundering and Terrorist Financing No. 20 of 2021 are fully consistent with the International Convention for the Suppression of the Financing of Terrorism 1999 and provide a more substantial framework for combating money laundering (AML) and countering terrorist financing (CFT), keep pace with developments and changes taking place in the world and at the same time ensure the protection of the national economy and the interests of all parties, to expand the scope of the categories covered by the provisions of the law, define the regulatory and supervisory bodies and competent authorities therein, expand the powers of the National Committee to Combat Money Laundering and Terrorist Financing, and define the tasks and powers of the unit.

The said committee is entitled to adopt and update procedures for assessing the risks of money laundering, terrorist financing and the proliferation of weapons of mass destruction in Jordan, provide the competent authorities with information related to risk assessments of money laundering and terrorist financing and strengthen cooperation and coordination in the field of applying the necessary frameworks to combat money laundering and terrorist financing, propose draft legislation related to money laundering and terrorist financing.

Article (4) in the new amended law aligned with FATF Recommendation (5), which identified the crime of financing terrorism and the material and moral elements for the occurrence of this crime. This article includes that any person can be considered to have committed a terrorist financing offense under the following circumstances:[32]

1. If they knowingly provide or collect funds, whether from legal or illegal sources, with the awareness that these funds will be used, either entirely or partially, to carry out a terrorist act by a terrorist or terrorist organization, directly or indirectly, through any means.
2. If they intentionally contribute to or support a group of individuals in committing a terrorist financing offense.
3. If they finance the travel of individuals to a country other than their own for the purpose of engaging in terrorist activities, planning, preparation, participation, or facilitation of terrorist acts, or for providing or receiving terrorist training.
4. If they participate in committing any of the terrorist financing offenses described in this paragraph, or if they organize or instruct others to commit such offenses.

5- If they attempt to commit any of the offenses outlined in this paragraph.

Furthermore, an offense of terrorist financing is considered to have been committed even if the terrorist act doesn't occur or isn't attempted. This holds true regardless of

[32] Anti-Money Laundering and Counter Terrorist Financing Law No. 21 of 2021.

whether the funds were actually used for the terrorist act, were connected to a specific terrorist act, or where the terrorist act was intended to take place.

The Financial Action Task Force emphasizes the adoption of a risk-based approach as a key recommendation to combat money laundering and terrorist financing effectively. This approach serves as a guide for countries to allocate resources and concentrate efforts on addressing high-risk deficiencies within their systems. Additionally, countries may opt to apply simplified measures in accordance with FATF recommendations for low-risk scenarios.

The importance of continuous and effective cooperation between various government agencies as part of the policy applied by the Central Bank of Jordan to monitor terrorist financing operations in accordance with a set of basic guiding principles in a way that contributes to achieving consistency and integrity in applying the risk-based supervision approach, since the risk-based approach achieves effective oversight of anti-money laundering and terrorist financing operations, which would provide the ability to respond to emerging threats and risks facing non-profit companies. In addition, this approach would contribute to help establish and sustain relationships based on cooperation with the stakeholders and encouraging effective and continuous compliance with anti-corruption requirements.

To implement FATF recommendation (1), the Unit led the works of a team formed by the competent authorities to execute what is mentioned in article (15) of the law. Such a team must identify, evaluate, comprehend, and oversee the entities' risks associated with money laundering and terrorist financing. This involves considering risk factors related to customers, countries, geographic areas, products, services, channels, transactions and evolving techniques. The assessment should be proportional to the reporting entity's nature and size, as well as in alignment with supervisory requirements and the national risk level.

Pursuant to article (22), the effective law ensures the importance of applying recommendation (24), which obliges the legal entities to file the beneficial owner in special records of the competent authorities. The law defines the term "beneficial owner" as it is "the natural person who ultimately owns or controls a customer, directly or indirectly or the person on whose behalf the transactions are being conducted or that ultimately controls a legal person or a legal arrangement".[33]

The new law formed the basic pillar in the field of Jordanian compatibility with international standards in the framework of combating money laundering and terrorist financing, in addition to amending other laws and legislation such as the Company Law, the beneficial owner registry system, and the accuracy of basic data related to companies. Such legislative reforms contributed to remove Jordan from the international list of countries under increased monitoring ahead of schedule, which reflects the commitment and high professionalism of Jordan in this field.

[33] Ibid.

5. Conclusion

Jordan exerted its efforts on enhancing the process of combating the financing of terrorism system and condemned all forms of terrorism, aligning itself with the international community's efforts and continually emphasized its dedication to combating terrorism, responding positively to requests for concrete actions in support of coalition initiatives against terrorists. This endeavor primarily serves the interests of Jordan, its economy, its financial system and contributes to the safety and security of its citizens.

In October, 2021, Jordan was announced to be under increased monitoring by FATF and pledged to promptly address the identified shortcomings within specified deadlines aimed at combating money laundering, terrorist financing, and proliferation financing. This roster is commonly known externally as the "grey list".

Recommendation (8) is one of the key FATF recommendations targeting Non-Profit Organizations and outlining the tools misused by terrorist groups including NPCs for purposes such as fundraising, facilitating the movement of funds, providing logistical assistance, recruiting individuals for terrorist activities, or otherwise supporting terrorist organizations and their operations. They may exist in various structures, such as a sole proprietorship (including personal charitable donations), an unincorporated association, a corporation, a foundation (characterized by its funding from a founder and organized as a trusteeship), or a condominium. Consequently, safeguarding the NPC sector from terrorist exploitation is not only vital in the global effort against terrorism but also essential for maintaining the integrity of such a sector and ensuring the trust of donors.

Consequently, such recommendations come to prevent the misuse of NPOs by terrorist organizations and measures should be implemented to[34] stop the exploitation of legitimate entities as channels for terrorist financing, including evading asset freezing measures and uncover and prevent the covert diversion of funds initially intended for legitimate purposes but redirected for terrorist activities.

The government of Jordan has embraced a strategy to rectify the deficiencies highlighted in the FATF mutual evaluation following an observation period. The plan involves implementing the action points within a specified timeframe, with FATF overseeing the progress of this implementation.[35]

Jordan must do legislative reforms and enhance the role of the supervisory authorities in countering all means utilized by the terrorists to legalize their illicit activities, particularly the policies implemented to protect non-profit companies from being abused. The importance of amending the legislation in Jordan lies in the importance of the legal texts related to combating the crime of money laundering and terrorist financing to dry up the sources of these crimes and prevent their occurrence.

Jordan has adopted the following measures to leave the grey list:

1. Amendment of the Anti-Money Laundering and Counter Terrorist Financing Law to criminalize terrorist financing, broaden the range of predicate offenses to include

[34] FATF 2001.

[35] Middle East & North Africa Financial Action Task Force 2009.

all crimes, grant greater independence to the Unit and expand the covered entities to include various financial institutions and non-financial businesses and professions.
2. Issuance and/or amendment of AML/CTF instructions and guidelines to a range of entities, including banks, money exchanges, insurance companies, securities firms, financial leasing companies, real estate, and jewelry businesses, by competent authorities.
3. Adoption of AML/CTF inspection manuals by the Central Bank of Jordan and the Insurance Commission.
4. Adoption of instructions and formalization of procedures for implementing obligations under UNSCRs 1267 (1999) and 1373 (2001).
5. Implementation of other measures by various competent authorities, such as the Companies Control Directorate adopting the Beneficiary Owner Declaration Form and the Ministry of Justice adopting Mutual Assistance Procedures and endorsing the Palermo Convention.
6. Understanding the associated risks and formulating appropriate mitigation measures are essential steps to deter and prevent criminals from exploiting legal persons and arrangements.
7. Maintaining comprehensive and up-to-date records of basic and beneficial ownership information for legal entities, monitoring and pursuing money laundering cases related to underlying offenses aligned with its risk profile, conducting risk-based monitoring of NPOs without impeding legitimate NPO activities, resulting in Jordan's official exemption from the FATF's heightened monitoring.

On October 27, 2023 the FATF plenary meeting concluded that Jordan is among the countries that had effectively addressed the action points outlined during the FATF onsite visit. Consequently, Jordan was deemed to have met the necessary criteria and removed from the grey list.

This announcement is considered as a recognition of Jordan's success in advancement in addressing its AML/CFT shortcomings and strengthens the national system to combat terrorist financing, harmonizing it with international standards contributing to strengthening its investment environment and completes the implementation of all provisions of the special action plan approved by (FATF) in October 2021.

The effective implementation of the plan is an imperative necessity to protect the economy and the region and to fully reap the benefits of Jordan's economic and financial activities.

The priority given by the government to combat money laundering and the financing of terrorism will not end with announcing this removal from the "grey list", but rather will continue in order to effectively address emerging issues related to combating money laundering and terrorist financing. Facing limitations in their legal authority to investigate, prosecute, and enforce anti-terrorist financing measures. This can hinder their ability to take decisive actions against suspicious activities.

Following the amendments made by Jordan recently, they are still under increased monitoring by FATF. There are no laws or measures that guarantee quick and effective responsiveness to mutual legal assistance. In general, the Unit, law enforcement agencies

and the supervisory authorities working in AML/CFT face limitations in their legal authority to investigate, prosecute, and enforce anti-terrorist financing measures. This can hinder their ability to take decisive actions against suspicious activities. Moreover, it lacks sufficient human, financial and technical resources to perform their duties effectively and employees of such authorities are not provided with appropriate training in relation to AML/CFT.

Ultimately, I recommend at the end of my article implementing one of the best practice tools, which is the adoption of good governance rules and strong financial management through appointing a Board of Directors having a high degree of understanding of the organization's goals and acting in their interest. The Board of Directors shall have the power to maintain and oversee the organization by establishing strong financial and human resources policies, meeting on a regular basis, and monitoring activities closely.

Bibliography

FATF, Combating the abuse of Non-Profit organizations (recommendation 8). Paris, 2015. https://www.fatf-gafi.org/media/fatf/documents/reports/BPP-combating-abuse-non-profit-organisations.pdf.

FATF, Money Laundering and Terrorist Financing Risk Assessment of Legal Persons and Legal Arrangements in Jordan. Paris, 2023. https://www.menafatf.org/sites/default/files/MER_Hashemite_Kingdom_of_Jordan.pdf.

FATF, IX Special Recommendations. Paris, 2001. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf.coredownload.pdf.

FATF, BPP-Combating the Terrorist Financing Abuse of Non-Profit Organisation. Paris, 2023. www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Bpp-combating-abuse-npo.html.

FATF, Guidance on the criminalisation of terrorist financing (Recommendation 5). Paris, 2016. www.fatf-gafi.org/publications/fatfrecommendations/documents/criminalising-terrorist-financing.html.

CGCC, To protect and prevent outcomes of a global dialogue to counter terrorist abuse of the nonprofit sector, 2013. https://www.globalcenter.org/wp-content/uploads/CGCC_Prevent-Protect-Report_pgs.pdf.

Middle East & North Africa Financial Action Task Force, Mutual Evaluation Report of the Hashemite Kingdom of Jordan. MENAFATF, 2009. https://www.menafatf.org/sites/default/files/MER_Hashemite_Kingdom_of_Jordan.pdf.

Anti-Money Laundering and Counter Terrorist Financing Law No. 21 of 2021.

FATF, Guidance on Beneficial Ownership for Legal Persons. Paris, 2023. http://www.fatf-gafi.org/publications/FATFrecommendations/guidance-beneficial-ownership-legalpersons.html.

FATF, The Hashemite Kingdom of Jordan's MER. Paris, 2019. https://www.menafatf.org/information-center/menafatf-publications/hashemitekingdom-jordan-mutual-evaluation-report.

DIGITAL CONTRACTING IN THE KYRGYZ REPUBLIC. EU LAW AS A ROLE MODEL FOR DEVELOPMENT

Akylbek Dzhusupov[1]

ABSZTRAKT ■ A digitális szerződési jog a Kirgiz Köztársaságban: az EU jog mint fejlesztési modell" című cikk a digitális szerződési környezetet mutatja be Kirgizisztánban, hangsúlyozva különböző jogi keretrendszerek alkalmasságát. Az összehasonlítás és elemzés alapjául a következőket választottam: az Egyesült Államok joga, mely vezető szerepet tölt be a gazdaság és technológia területén, az Európai Unió joga erős gazdasági fejlettségű régióként hatalmas történelmi és jogi háttérrel rendelkezik a szabályozásban, a nemzetközi jog pedig, mint a világgazdaság minden kapcsolatának általános szabályozója, a legjobb világgyakorlatokat gyűjti össze. Ez az összehasonlító nézőpont kiemelheti bizonyos jogi keretrendszerek erősségeit, gyengeségeit és egyedi jellemzőit, értékes betekintést nyújtva az olvasók számára. Ezen kívül a cikk tartalmazza a kirgiz jogszabályok szerződésekre vonatkozó rendelkezéseit és azok digitális eszközökkel történő végrehajtásának lehetőségeit. Az utóbbi években Kirgizisztán jelentős előrelépéseket tapasztalt a technológia és a digitális infrastruktúra terén. Az internetes szolgáltatások széles körű elérhetősége és a digitális technológiák egyre szélesebb körű elfogadása kedvező környezetet teremt a digitális szerződések lebonyolításához. Mint fejlődő gazdaság, a Kirgiz Köztársaság szorgalmazza a gazdasági növekedést és fejlődést. A digitális szerződések elfogadása elősegítheti az üzleti folyamatok egyszerűsítését, a tranzakciós költségek csökkentését és külföldi befektetéseket vonzhat, ezáltal hozzájárulva a gazdasági jóléthez.

Az Egyesült Államok és az Európai Unió jogi rendelkezéseinek, valamint a nemzetközi szervezetek modelljogának összehasonlító elemzése mellett a cikk hangsúlyozza az EU jogának előnyeit, mint amely a legalkalmasabb minta a Kirgiz Köztársaság jogalkotásához. Az EU jogot általában átfogónak, jól kifejlesztettnek és a demokrácia, az emberi jogok és a fogyasztóvédelem elveire épülőnek tartják. Erős keretrendszert biztosít különféle jogi területeken, beleértve a kereskedelmet, a környezetvédelmet és a fogyasztói jogokat. Emellett az EU jogot évtizedek óta átfogó vizsgálatnak, finomításnak és igazításnak vetik alá, ami egy fejlett jogrendszerhez vezet, és számos napi kihívást képes kezelni.

Végül az EU jog fejlesztési modellként történő elfogadása elősegítheti a digitális szerződéskötés fejlődését, valamint összehangolhatja azt a globális szabványokkal, ezzel lehetővé téve a Kirgiz Köztársaság számára a globális gazdaságba való jobb integrációt.

[1] PhD student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

ABSTRACT ■ The article "Digital Contracting in the Kyrgyz Republic: EU Law as a Role Model for Development" explores the landscape of digital contracting in Kyrgyz Republic, focusing on the suitability of legal frameworks from various jurisdictions. I chose the following as the basis for comparison and analysis: The United States' Law as a leading country in economy and technology, European Union Law as a strong economically developed region with a huge historical legal background in regulation and international law as a general ruler of all relationships of the world economy which gathers best world practices. This comparative perspective can highlight strengths, weaknesses and unique features of certain legal frameworks, providing valuable insights for readers.

Also, this article contains the provisions of the Kyrgyz legislation regarding the contracts and opportunities enforcing them by digital means. In recent years, Kyrgyzstan has experienced notable progress in technology and digital infrastructure. The widespread accessibility of internet services and the increasing adoption of digital technologies have established a favorable environment conducive to the implementation of digital contracts. As a developing economy, the Kyrgyz Republic is keen on fostering economic growth and development. Embracing digital contracts can streamline business processes, reduce transaction costs, and attract foreign investment, thereby contributing to economic prosperity.

Through a comparative analysis of legal provisions from US and EU Law, as well as the model law of international organizations, the article underscores the advantages of adopting EU Law as the most fitting model for legislation in the Kyrgyz Republic.

EU law is often considered comprehensive, well-developed, and grounded in principles of democracy, human rights, and consumer protection. It provides a robust framework for various legal aspects, including trade, environmental protection, and consumer rights. Additionally, EU law has been the subject to extensive scrutiny, refinement, and adaptation over decades, resulting in a sophisticated legal system that addresses many contemporary challenges.

Ultimately, adopting EU Law as a model for development could facilitate the growth of digital contracting and align with global standards, positioning the Kyrgyz Republic for enhanced integration into the global economy.

Kulcsszavak: digitalizálás, digitális szerződés, Kirgiz Köztársaság, EU jog, elektronikus aláírás

1. Introduction

As an experienced lawyer in the business sector, who is interested in the integration of the Kyrgyz Republic to the global market, I decided to research all of the legal environment in digital contracting of the advanced countries and unions.

I believe that the study will address the existing gap in knowledge regarding the legal aspects of digital contracting in the Kyrgyz Republic and the potential benefits of aligning with leading legislation. It will contribute to the understanding of the legal requirements and implications for the Kyrgyz Republic's economic integration. By recommending legal reforms and adaptations based on advanced rules, the study aims to facilitate the Kyrgyz Republic's economic integration into the global market. Aligning legislation with EU or US standards can create a more favorable environment for cross-border business transactions and attract foreign investments.

A well-defined legal framework for digital contracting can remove barriers and provide legal certainty to businesses engaged in international trade. The study's recommendations will help the Kyrgyz Republic create an enabling environment for businesses to participate in the global market and foster international trade relationships. Also, the study's findings and recommendations will contribute to strengthening the rule of law in the Kyrgyz Republic by promoting transparency, fairness, and legal certainty in digital commercial relationships. It will help create a predictable legal environment that protects the rights and legitimate interests of businesses and consumers. Additionally, the study will provide an alternative opinion to the government of the Kyrgyz Republic in its efforts to enhance the legislative framework for digital contracting.

2. The research question and objectives of the article

I put the research question as follows:
"What legal reforms and adaptations are necessary in the Kyrgyz Republic to align its legislation with global trend laws and regulations on digital contracting, and how can this alignment enhance economic integration and participation of the Kyrgyz Republic in the global market?"

For the purpose of finding an answer for my research questions I have identified several objectives and analyzed the current legal framework for digital contracting in the Kyrgyz Republic, including relevant laws, regulations, and policies. Additionally, there was a need to examine International, US and EU laws and regulations pertaining to digital contracting and identify key provisions that can serve as a benchmark for the Kyrgyz Republic and I compared and assessed the similarities and differences between the legal frameworks of them regarding digital contracting in order to find best law which will help my country to be part of world business.

Moreover, I tried to identify areas where the legislation of the Kyrgyz Republic needs to be amended or adapted to align with world standards and best practices. Providing recommendations to the government of the Kyrgyz Republic on necessary legal reforms and adaptations to enhance the legal framework for digital contracting, drawing consequences from the rules and experiences of the leading economies, was another challenge for me.

3. Legal analysis of regulations in digital contracting

Numerous regulations worldwide govern digital contracts, but determining the most suitable one for the Kyrgyz Republic remains a crucial question.

Situated in the heart of Central Asia, Kyrgyzstan is a landlocked country with a population exceeding 7 million. It shares borders with the People's Republic of China to the east, Kazakhstan to the north, Uzbekistan to the west, and Tajikistan to the southwest. Spanning 199,951 square kilometers, its terrain is primarily mountainous, with approximately 94% of the country lying above 1,000 meters and 40% above 3,000 meters. The currency is the som (KGS), and Kyrgyz and Russian serve as the official languages[2]. As a newly independent nation, Kyrgyzstan is poised to embrace various challenges, prompting a comprehensive exploration of European Union law, United States law, and international law to identify the most suitable regulatory framework.

3.1. EU legislation on digital contracting

The evolution of regulations pertaining to digital contracting commenced with the enactment of Directive 1999/93/EC by the EU Parliament and Council on December 13, 1999. The aim of this directive is to streamline the adoption of electronic signatures and enhance their legal validity. It lays down a regulatory framework for electronic signatures and specific certification services to uphold the effective operation of the internal market[3]. This directive introduces new terminology such as "electronic signature", "signature-creation data", "signature-verification device", "certificate", and "electronic-signature product".

[2] National Investments Agency under the President of the Kyrgyz Republic: General information about Kyrgyz Republic. https://invest.gov.kg/about-kyrgyz-republic/general-information/.

[3] Directive 1999/93/EC of the EU Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures. OJ L 13, 19.1.2000,12-20.

Member States were tasked with ensuring that advanced electronic signatures, employing a qualified certificate and produced by a secure signature creation device, meet the legal criteria for electronic data signatures, mirroring the validity of handwritten signatures for paper-based data. Additionally, these electronic signatures should be recognized as permissible evidence in legal proceedings.

The European Parliament's resolution of 21 September 2010[4] on completing the internal market for e-commerce, stressed the importance of the security of electronic services, especially of electronic signatures and of the need to create a public key infrastructure at pan-European level and invited the Commission to set up a European validation authorities gateway to ensure the cross-border interoperability of electronic signatures and to increase the security of transactions carried out using the internet.

Next, it was the European Council's turn. Through its conclusions on February 4, 2011, and October 23, 2011, the Council urged the Commission to establish a digital single market by 2015, advance swiftly in key digital economy areas and foster a fully integrated digital single market by easing cross-border utilization of online services. Special emphasis was placed on facilitating secure electronic identification and authentication.

In numerous cases, EU citizens faced obstacles in using their electronic identification for authentication across different Member States due to the lack of recognition of national electronic identification schemes. This electronic barrier not only impedes service providers from fully leveraging the internal market's benefits but also complicates cross-border operations for businesses dealing with public authorities. The endorsement of mutually acknowledged electronic identification methods will facilitate seamless cross-border service provision within the internal market and streamline business operations across borders.

In accordance with the provisions of Directive 1999/93/EC, measures were proposed by the Commission to promote cross-border certification services and legal acknowledgment of advanced electronic signatures from third countries. The Commission was advised to ensure effective implementation of relevant standards and international agreements for certification services. Additionally, where necessary, the Commission was encouraged to present proposals to the Council, seeking mandates for negotiations of agreements with third countries and international organizations.

Following the proposal from the European Commission, the European Parliament and the Council of the European Union adopted the Regulation

[4] Completing the internal market for e-commerce European Parliament resolution of 21 September 2010 on completing the internal market for e-commerce (2010/2012(INI)). OJ C 50E, 21.2.2012, 1-15.

(EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC[5] (eIDAS Regulation), which establishes a framework for electronic identification and trust services for electronic transactions in the internal market. This Regulation enhances and expands the acquis of the Directive 1999/93/EC. According to Article 1, eIDAS Regulation:

a) lays down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;
b) lays down rules for trust services, in particular for electronic transactions; and
c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

The second crucial aspect for the contract's enforceability involves identifying the parties involved. As per the eIDAS Regulation, the aim is to strengthen trust in electronic transactions within the internal market, establishing a common foundation for secure electronic interactions among individuals, businesses, and governmental bodies. This endeavor is anticipated to boost the effectiveness of both public and private online services, electronic business, and e-commerce throughout the European Union. However, it's noteworthy that this Regulation does not alter national or Union laws concerning the conclusion and validity of contracts, or other legal or procedural requirements related to their form. The eIDAS certification delineates standards and criteria for various electronic signature types, qualified certificates, and online trust services. Furthermore, it rules electronic transactions and their management[6].

The third essential part of the digital contracting is ensuring parties to protect personal data. The contract of B2C type means that one party is always a natural person. For the purpose of protecting personal data the EU adopted General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with

[5] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, 73-114.

[6] Alba Zaragoza: eIDAS. The Digital Identification Regulation for Europe. The Signicat Blog, 17.07.2023, https://www.electronicid.eu/en/blog/post/eidas-regulation-electronic-signature/en.

regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)[7].

Processing shall be lawful only if it is necessary for the performance of a contract to which the natural person is party or in order to take steps at the request of the natural person prior to entering into a contract[8]. Naturally, obtaining the consent of the data subject for processing their personal data for specific purposes is a mandatory requirement. In this context, digital contracts offer distinct advantages over other contract types, as they allow consumers to simultaneously provide consent for personal data processing when signing. When assessing the voluntary nature of consent, special attention should be paid to whether agreeing to process personal data, which isn't integral to fulfilling a contract, it is a prerequisite to execute the contract or receive a service.

Regulation (EU) 2016/679, commonly known as the GDPR, or any other relevant Union law on data protection, should fully apply to the processing of personal data in relation to contracts in Europe. It is important to note that the further mentioned Directives do not undermine the rights, obligations and non-contractual remedies established by GDPR.

Failure to adhere to the stipulations outlined in Regulation (EU) 2016/679, which encompass fundamental principles such as data minimization, data protection by design, and data protection by default, may, depending on the circumstances, also result in noncompliance with the subjective or objective conformity requirements specified in other legislative acts. For instance, if a trader explicitly undertakes an obligation within a contract, or if such an obligation can be inferred from the contract's terms, relating to the trader's responsibilities under the GDPR, this contractual commitment may constitute part of the subjective conformity requirements. Similarly, noncompliance with GDPR obligations that renders digital content or services unsuitable for their intended purpose can also lead to a lack of conformity with the objective requirement for compliance. This objective requirement mandates that digital content or services be fit for their typical usage purposes when compared to other digital content or services of a similar nature.

In essence, the application of data protection regulations to the processing of personal data within relevant contracts is obligatory. Noncompliance with GDPR obligations can impact the assessment of conformity for digital content

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, 1-88.

[8] Article 6(1) GDPR.

or services, considering both subjective contractual commitments and objective suitability for purpose requirements.

To solve the problems of protecting consumer rights, harmonising national contract law and improving cross-border trade, the European Parliament and the Council by the proposal of the European Commission on 20 May 2019 adopted Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services[9] and Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods[10].

The application of Directive (EU) 2019/770, which pertains to contracts for the supply of digital content and digital services, and Directive (EU) 2019/771, which focuses on contracts for the sale of goods, commenced on 1 January 2022. These directives aim to harmonize crucial rules governing consumer contracts throughout the European Union, resulting in a robust level of consumer protection and enhanced legal certainty for both consumers and traders engaged in countless everyday transactions involving goods, smart goods, digital content, and digital services.

The freedom of choice. According to Article 3(1) Convention on the law applicable to contractual obligations opened for signature in Rome on 19 June 1980 (80/934/EEC) (Rome Convention): *"A contract shall be governed by the law chosen by the parties. The choice must be expressed or demonstrated with reasonable certainty by the terms of the contract or the circumstances of the case. By their choice the parties can select the law applicable to the whole or a part only of the contract"*. The parties' freedom to choose the applicable law considered one of the cornerstones of the system of conflict-of-law rules in matters of contractual obligations according to the European Parliament and the Council of European Union. Therefore, in Rome I[11] regulation there is an article (#3) with the same text. Thus, digital contracts are in harmony with private international law.

Moreover, the aforementioned Regulation should not impede the implementation of other mechanisms that contribute to the effective operation of the EU internal market. If these mechanisms cannot coexist with the law designated by the provisions of the Rome-I regulation, they should still be respected. The application of the designated applicable law should not obstruct the free movement of goods

[9] Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services. OJ L 136/1, 22.5.2019.

[10] Directive (EU) 2019/770 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC. OJ L 136/28, 22.5.2019.

[11] Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). OJ L 177, 4.7.2008, 6-16.

and services as governed by Union instruments, such as Directive 2000/31/EC concerning legal aspects of information society services, including electronic commerce, within the Internal Market. Additionally, this regulation does not prohibit parties from incorporating nondomestic laws or international conventions into their contract through referencing. Therefore, it is a favorable condition for the parties to choose for instance: the International Institute for the Unification of Private Law (UNIDROIT)[12], HCCH (Hague Conference on Private International Law – Conférence de La Haye de droit international privé)[13] or United Nations Convention on Contracts for the International Sale of Goods (CISG). Principles as the rules of law governing their contract or, in case of a dispute, as the rules of law applicable to the substance of the dispute. According to István Erdős, Assistant professor and Lecturer the Department of International Private Law and European Economic Law at Eötvös Loránd University: *"It means in the present case that choosing directly the CISG would be considered as a choice of rules of law under the Rome I regulation..."*[14].

3.2. Legal analysis of US laws and regulations relevant to digital contracting

In the United States, the Uniform Electronic Transactions Act (UETA)[15] and the Electronic Signatures in Global and National Commerce Act (ESIGN)[16] define and govern digital contracts. UETA has been adopted almost by all states, and ESIGN is a federal law that applies to interstate and foreign commerce.

12 *"The UNIDROIT Principles provide a balanced set of rules covering virtually all the most important topics of general contract law, such as formation, interpretation, validity including illegality, performance, non-performance and remedies, assignment, set-off, plurality of obligors and of obligees, as well as the authority of agents and limitation periods"*. UPICC Model Clauses for the use of the UNIDROIT Principles of international commercial contracts. https://www.unidroit.org/instruments/commercial-contracts/upicc-model-clauses/#:~:text=The%20UNIDROIT%20Principles%20provide%20a,obligees%2C%20as%20well%20as%20the.

13 *"The HCCH's mission is to resolve these questions by providing internationally agreed solutions, developed through the negotiation, adoption, and operation of international treaties, the HCCH Conventions, to which States may become Contracting Parties, and soft law instruments, which may guide States in developing their own legislative solutions"*. https://www.hcch.net/en/about.

14 István Erdős: *Private International Law in Business Transactions. Contracts Non-contractual obligations.* Budapest, 2016 (https://edit.elte.hu/xmlui/handle/10831/30613).

15 Uniform Electronic Transaction Act (UETA) of the United States of America. https://www.uniformlaws.org/viewdocument/final-act-21?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034&tab=librarydocuments.

16 Electronic Signatures in Global and National Commerce Act (ESIGN) of the United States of America. https://www.govinfo.gov/content/pkg/PLAW-106publ229/html/PLAW-106publ229.htm.

ESIGN signed into law on June 30, 2000, provides a general rule of validity for electronic records and signatures for transactions in or affecting interstate or foreign commerce. The E-Sign Act allows the use of electronic records to satisfy any statute, regulation, or rule of law requiring that such information be provided in writing, if the consumer has affirmatively consented to such use and has not withdrawn such consent[17].

The ESIGN Act affirms that electronic signatures carry equivalent legal weight to traditional ink-on-paper signatures. This law offers significant cost savings for businesses by minimizing expenses related to mailing and processing physical copies of contracts and associated documents. Additionally, the ESIGN Act confirms the legitimacy of electronic records and signatures in transactions spanning interstate and international commerce. According to this legislation, electronic signatures are subject to the same standards and legal scrutiny for authenticity as their paper-based counterparts.

According to ESIGN, "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities and the term "Contract" included as a part of the definition for "Electronic record". Particularly, it says that the term "electronic record'" means a contract or other record created, generated, sent, communicated, received, or stored by electronic means[18]. Thus, we can say that a contract created by technology capabilities may be considered as "a digital contract".

UETA provides uniform rules governing electronic commerce transactions. It sets a legal foundation for the use of electronic communications in business transactions where the parties have agreed to deal electronically. UETA validates and supports the use of electronic communications and records and places electronic commerce and paper-based commerce on the same legal footing. According to UETA, the term "Electronic" has the same meaning as in ESIGN and "contract" means the total legal obligation resulting from the parties' agreement[19]. Therefore, we can consider that a digital contract is "an agreement created and signed by electronic means". The act is designed to facilitate and promote commerce and governmental transactions by validating and authorizing the use of electronic records and signatures and to promote uniform electronic

[17] Federal Deposit Insurance Corporation FDIC: Consumer Compliance Examination Manual – January 2014. https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/10/x-3-1.pdf.

[18] Section 106, ESIGN.

[19] Section 2, UETA.

transaction laws among the states. It is also designed to be consistent with other applicable laws[20].

The fundamental messages of the UETA are:

- a record or signature may not be denied legal effect or enforceability solely because it is in electronic form;
- a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation;
- an electronic record satisfies a law that requires a record to be in writing;
- an electronic signature satisfies a law that requires a signature.

3.3. Legal analysis of international laws and regulations relevant to digital contracting

As one of the fundamental laws for all countries including the Kyrgyz Republic and Member states of European Union is certainly the Model Law of United Nations Commission on International Trade Law (UNCITRAL).

It started in 1996 when UNCITRAL adopted the Model Law on Electronic Commerce (MLEC)[21] that aims to enhance and simplify electronic commerce by offering a standardized set of rules that can be adopted by national legislators. These rules are designed to eliminate legal barriers and enhance legal predictability in electronic commerce transactions. One of the key objectives of the MLEC is to address challenges arising from statutory provisions that cannot be altered through contractual agreements. By providing equal treatment to both paper-based and electronic information, the MLEC promotes the use of paperless communication, which in turn fosters efficiency in international trade. By establishing a consistent legal framework, the MLEC facilitates electronic commerce and promotes harmonization across jurisdictions.

Then on 5 July 2001 UNCITRAL adopted the Model Law on Electronic Signatures (MLES)[22]. The growing reliance on electronic authentication methods as alternatives to traditional handwritten signatures and other authentication

[20] Sandra Norman-Eady: Uniform Electronic Transaction Act. *Old Research Report,* 2000-R-1076. https://www.cga.ct.gov/2000/rpt/2000-R-1076.htm.

[21] United Nations Commission on International Trade Law: *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998*. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf.

[22] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf.

procedures has highlighted the necessity for a dedicated legal framework that addresses the legal implications of using electronic means. In response to these requirements, the MLES builds upon the fundamental principle outlined in the MLEC. This principle pertains to the fulfillment of the signature function in an electronic environment and adopts a technology-neutral approach. By avoiding favoritism towards any specific technology or process, the MLES enables legislation based on this Model Law to recognize various types of electronic signatures, including digital signatures based on cryptography as well as electronic signatures utilizing alternative technologies. This approach ensures that the legal framework remains adaptable to different authentication methods and promotes flexibility in the use of electronic signatures.

Therefore, the aim of the MLES was to enable and facilitate the use of electronic signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures. Thus, the MLES may assist States in establishing a modern, harmonized and fair legislative framework to address effectively the legal treatment of electronic signatures and give certainty to their status.

The MLES is grounded in the fundamental principles shared by all UNCITRAL texts concerning electronic commerce. These principles include nondiscrimination, technological neutrality, and functional equivalence. The MLES sets out criteria for assessing the technical reliability necessary to equate electronic signatures with handwritten signatures. It also establishes fundamental rules of conduct that can serve as guidance when determining the obligations and liabilities of signatories, relying parties, and trusted third parties involved in the signature process. Additionally, the MLES includes provisions that promote the recognition of foreign certificates and electronic signatures, following a principle of substantive equivalence that disregards the origin of the signature. This approach facilitates cross-border transactions and fosters international cooperation in recognizing the legal validity of electronic signatures.

After that in 2017 UNCITRAL decided to adopt Model Law on Electronic Transferable Records (MLETR)[23]. This step was done in order to enable the legal use of electronic transferable records both domestically and across borders. The MLETR applies to electronic transferable records that are functionally equivalent to transferable documents or instruments. Transferable documents or instruments are paper-based documents or instruments that entitle the holder to claim the performance of the obligation indicated therein and that allow the transfer of

[23] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Transferable Records. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf.

the claim to that performance by transferring possession of the document or instrument. Transferable documents or instruments typically include bills of lading, bills of exchange, promissory notes and warehouse receipts.

Finally, on 7 July 2022 UNCITRAL adopted the Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT)[24]. The purpose of this Law is to provide a standardized set of legislative provisions that enable the legal use of identity management services for online identification of individuals and entities, as well as the use of trust services to ensure the quality of electronic data. Additionally, the MLIT establishes mechanisms for facilitating the cross-border recognition of identity management and trust services.Digital trade requires trust in the identity of commercial partners and the quality of electronic data. Identity management services verify the online identification of individuals and entities, while trust services certify the quality of data. These services are typically provided by specialized third parties. The MLIT sets a uniform legislative standard to promote trust in digital transactions and documents. As the first global legislative text of its kind, it serves as a legal foundation for digital trade worldwide, complementing other UNCITRAL legislative texts related to electronic commerce.

Chapter I defines relevant terms, outlines the scope of application, and establishes general provisions regarding the voluntary use of identity management and trust services, as well as their relationship with other laws.

Chapter II establishes the fundamental elements of the legal framework applicable to identity management. It outlines core obligations for identity management service providers and subscribers and sets rules regarding the liability of identity management service providers. Notably, Article 9 introduces a key provision on functional equivalence, which states that offline identification and identification conducted through identity management must be functionally equivalent and rely on a reliable method. The reliability of the method is assessed either retrospectively based on the circumstances or prospectively through designation.

Chapter III establishes the foundational elements of the legal framework for trust services, including provisions regarding the liability of trust service providers. Articles 16 to 21 specify the functions of certain trust services (e.g., electronic signatures, electronic seals, electronic timestamps, electronic archiving, electronic registered delivery services, and website authentication) and the associated requirements. Similar to identity management, the reliability

[24] United Nations Commission on International Trade Law, UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mlit_advance_copy.pdf.

of the method used for trust services is assessed retrospectively based on the circumstances outlined in Article 22 or prospectively through designation as per Article 23.

Chapter IV focuses on enabling the cross-border recognition of identity management and trust services, a key objective of the Model Law. It employs a decentralized approach and utilizes both retrospective and prospective mechanisms for assessing the reliability of the methods employed.

The United Nations Convention on Contracts for the International Sale of Goods (CISG) applies to contracts of sale of goods between parties whose places of business are in different States. Neither the nationality of the parties nor the civil or commercial character of the parties or of the contract is to be taken into consideration in determining the application of this Convention.

The CISG is also complemented, with respect to the use of electronic communications, by the United Nations Convention on the Use of Electronic Communications in International Contracts, 2005 (the Electronic Communications Convention). The Electronic Communications Convention aims at facilitating the use of electronic communications in international trade by assuring that contracts concluded and other communications exchanged electronically are as valid and enforceable as their traditional paper-based equivalents[25].

3.4. The Kyrgyz Republic's legislation on digital contracting

Contracts: Article 395 (1) of the Civil code of the Kyrgyz Republic[26] prescribes: *"A contract may be entered into in any form provided for making transactions, unless the law establishes a specific form for such type of a contract. If the parties agree to enter into a contract in a certain form, it shall be deemed as entered into from the time it was structured in such form, even though such form is not required by law for such type of a contract"*. These rules ensure the different participants of civil relationship to use any kind of form of the contract, unless such kind of contracts are obligatory by the law. For instance, when it comes to a purchase agreement for real estate, it must be formalized in writing and undergo state registration with specific agencies. This requirement is a mandatory rule that everyone must adhere to.

[25] United Nations Convention on Contracts for the International Sale of Goods. New York 2010. (31) https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-09951_e_ebook.pdf.

[26] Europäisches Institut GmbH (European Institute), The unofficial translation of the Civil code of the Kyrgyz Republic. https://www.libertas-institut.com/de/Mittel-Osteuropa/Civil%20Code%20part%20I.pdf.

However, in other types of relationships, you have the flexibility to choose the format you prefer, hence digital contracts are permissible.

Moreover, a contract in a written form may be entered into by drawing a single document signed by the parties, and by exchanging letters, telegrams, teletypes, telephoned telegrams, through fax or electronic or other communication or by other means which allow to establish authentically that the document derives from the contracting parties (Art. 395 (2))[27]. Through these provisions, the legislators of the Kyrgyz Republic have granted permission for both legal entities and individuals to utilize not only traditional paper-based written contracts but also to create a single electronic document that can be signed by both parties. The crucial aspect is ensuring clarity regarding the identity of the signatories to the contract.

"A transaction shall be made in written form by creation of a document which expresses the substance of the transaction and is signed by the person or persons making the transaction, or by persons properly authorized by them. Bilateral transactions may be made by exchanging of documents, each signed by the party which originates it (paragraph 2 of Article 395)".

Electronic signature: The Civil code of KR also provides a regulation on enforcing a contract which signed by the electronic signature. Pursuant to Art. 176 (2): *"A facsimile reproduction of a signature by means of mechanical or other copying, electronic signature or any other analogue of a personal signature is permitted if provided for by law or by agreement of the parties".*

The electronic signature plays a crucial role in digital contracting, as it is essential for finalizing contracts using remote acknowledgment tools. Just as handwritten signatures are commonly used in paper-based contracts, electronic signatures serve the same purpose in digital contracts. According to the Law of the Kyrgyz Republic on Electronic Signature № 128 as of July 19, 2017 (Law on Electronic Signature) this Law governs the relations on use of digital signatures when making civil transactions, rendering the state and municipal services, execution of the state and municipal functions, and also when making legally significant actions.

As it described in Article 2 of the Law on Electronic Signature the digital (electronic) signature (ES) - information electronically, which is attached to other information electronically and (or) is logically connected with it and which is used for determination of person on behalf of which information is signed[28].

[27] The original version of the Civil code of the Kyrgyz Republic is available on website http://cbd.minjust.gov.kg/act/view/ru-ru/4/730?cl=ky-kg&mode=tekst.

[28] The unofficial translation of the Law of the Kyrgyz Republic on Electronic Signature № 128 as of July 19, 2017. https://cis-legislation.com/document.fwx?rgn=99019.

This Law allows the usage of two types of the electronic signature:
– Simple electronic signature;
– Advanced electronic signature (qualified, unqualified).

As per the Electronic Signature Law, individuals are authorized to utilize the basic ES, as it can be represented in the form of codes or encryption, thereby holding the same legal weight as signing a document by hand. Conversely, the advanced ES holds equivalent legal validity to handwritten signatures coupled with official stamps, making it more appropriate for use by legal entities.

Court procedures: The Civil Procedural Code of the Kyrgyz Republic recognizes electronic document and contract as a written proof by allocating that *"acts, documents, agreements, invoices, business correspondence and materials received through fax, electronic or any other communication device, the authenticity of which is proven, will be accepted as a written proof"*[29]. Besides this, the legal act of the Cabinet of Ministers allows the parties to verify the websites by a notary in order to prove the existing file on a certain time and date. Particularly, a testimony of a copy of Internet pages is allowed. For this purpose, the notary examines the information posted on the Internet. The Internet page shall be completely printed on paper and it is mandatory to indicate the date of printing and the link of the webpage, set in automatic mode. After printing, the written version shall be compared with the electronic version[30] (Art. 156 Instruction for performing notarial acts by notaries of the Kyrgyz Republic).

According to Article 428: *"In the Kyrgyz Republic, foreign court decisions, including those related to the approval of amicable agreements, are acknowledged and enforced if they are in accordance with the laws or international agreements that have been duly ratified and accepted by the Kyrgyz Republic or based on the principle of reciprocity"*[31].

[29] Civil Procedural Code of the Kyrgyz Republic, Article 80(1).

[30] The original version of Article 156 of the Instruction for performing notarial acts by notaries of the Kyrgyz Republic: *"Veb-sayttın köçürmösün kübölöndürüügö uruksat berilet. Oşol ele uçurda notarius İnternette jaygaştırılgan maalımattı tekşeret: İnternet barakçası basılgan künün jana fayldın daregin mildettüü türdö körsötüü menen avtomattık türdö kagazga tolugu menen basılıp çıgat. Basma versiyası çıkkandan kiyin elektronduk versiyası menen salıştırılat.Kübölöndürüü jazuusunda notarius İnternettegi barakçanın daregin, dokumenttin daregin, zarıl bolgon uçurda maalımattın atalışın, teksttik je grafikalık maalımatın, anın İnternet barakçasında jaygaşkan jerin körsötöt"*. (http://cbd.minjust.gov.kg/act/view/ru-ru/95038/65?cl=ky-kg&mode=tekst).

[31] Civil Procedural Code of the Kyrgyz Republic. The original version is available on official website http://cbd.minjust.gov.kg/act/view/ru-ru/111521?cl=ru-ru.

4. Main findings and arguments presented in the article

One of the barriers to trade in the Kyrgyz Republic is the lack of using electronic tools. Therefore, even in the report of the United Nations Economic Commissions for Europe seven years ago there was the following recommendation: Ensure the implementation of the law "On Electronic Document and Digital Signature". Immediate steps, as suggested by some State officials, include amending the laws governing the procedures and activities of individual State agencies, with a view to provide clear guidelines for implementing digital signatures. State agencies should also receive advanced training in this area, and equipped with the required tools and management information systems to ensure data storage security[32].

Before 2014, in many instances across the European Union, individuals from one Member State were unable to utilize their electronic identification to authenticate themselves in another Member State due to the lack of recognition of their national electronic identification schemes. This electronic barrier prevented service providers from fully leveraging the advantages of the internal market. Given the substantial similarities between European Union Law and the legal system of the Kyrgyz Republic, it is advisable to draw insights from leading countries' experiences. Consequently, it is recommended that the lawmakers of the Kyrgyz Republic permit the use of electronic identification from foreign countries. The mutual recognition of electronic identification means will streamline the cross-border provision of various services within the internal market and facilitate businesses' cross-border operations by minimizing hurdles in interactions with public authorities.

"The parties may at any time agree to subject the contract to a law other than that which previously governed it, whether as a result of an earlier choice under this Article or of other provisions of this Convention" (Article 3(2) Rome Convention 19 June 1980). This is the most useful advantage in digital contracts, because when you have access to internet you can make amendments to a contract any time. It is applicable even when you want to change the governing law.

One of the challenges we face is the absence of a legal framework for presenting evidence. Currently, the courts in the Kyrgyz Republic only recognize paper-based evidence during legal proceedings. Electronic files are not accepted because trial case files consist solely of documents in paper format. Moreover, parties are unable to simply print the required documents and authenticate them with

[32] United Nations Economic Commission for Europe, Regulatory and Procedural Barriers to Trade in Kyrgyzstan Needs Assessment. United Nations, New York and Geneva, 2015. 21. https://unece.org/DAM/trade/Publications/ECE_TRADE_412E-Kyrgyzstan.pdf.

a stamp. Hence, it is imperative to enhance the civil procedural legislation by incorporating regulations for collecting files not only in paper format but also electronically.

Another important part of the contacts is payment issue. In that regard, European authorities pay close attention to electronic payment (e-payment), which is a process of paying for transactions without using cash by using an e-payment system or medium instead. It is too hard to imagine that someone will use cash when concluding a contract through electronic means. The use of e-payment has expanded as the use of internet-based banking and e-commerce has grown. In modest international commercial transactions, e-payment frequently replaces using a credit or debit card[33].

I would like to note that not all legal implementations will be successful. New digital rules should be accepted by the market, and especially by the big tech players around the world, particularly by European ones. In his article "The Rise and Fall of Common European Sales Law", Miklós Király, Head of Department and Professor of Private International Law and European Economic Law and former Dean of ELTE University Faculty of Law, Member of Expert Group on a Common Frame of Reference in the area of European Contract Law, shared his predictions. *"Despite all these uncertainties, one day the project of European contract law may come back to the legislative agenda. The idea is not completely forgotten; the CESL remains one of the reference texts for European contract law. The forty year long history of the preparation of the Statute of the European Company (SE), which quite suddenly brought results, may console those who supported and still support the development of CESL. However, in order to achieve this goal, political and institutional support and clear and visionary guidance are needed. The fate of European contract law depends on the institutional dynamics and future of the EU, too"*[34].

5. Discussing the implications of the research for the Kyrgyz Republic's economic integration into the global market

Recent developments in digital technology illustrate the enormous benefits that can be derived if domestic and international trade and trade finance were to be undertaken digitally, in line with the increasing use of digital communications in commerce around the world. However, a significant barrier to digitalise trade

[33] Narmin Miriyeva: European Payments in the Digital Age. *ELTE Law Journal,* 2/2022..
[34] Miklós Király: The Rise and Fall of Common European Sales Law. *ELTE Law Journal, 2/2015.*

and trade finance is presented by outdated laws in many countries[35]. This article presents a compelling argument for embracing digital trade, contrasting some of the legal differences between regions that prevail worldwide with the much faster, simpler, more secure, and environmentally friendly digital trade processes that modern technology offers. It is my personal view that the government of the Kyrgyz Republic can modernize national laws by introducing new tools and approaches to digitalize business operations and eliminate legal barriers to digital trade and trade finance.

The laws mentioned in this article developed different kind of acts and regulations which help the developing countries to adopt the new fundamental rules and principles, which can help them to foster the integration into the global market. However, since EU Law has more balanced legal environment and similarities, the best way for the integration of the Kyrgyz Republic to the global market is to accept the research and model laws of the EU and incorporate them into the national law.

To achieve a genuine digital market and promote consumer protection, it is necessary to harmonize specific aspects of contracts for the supply of digital content or digital services. This harmonization should be based on a high level of consumer protection, aiming to enhance legal certainty and minimize transaction costs, particularly for Central Asia's small and medium-sized enterprises. Consumer rights hold significant importance in both Kyrgyz Law and the legal structure of Europe, as they view consumers as the "weaker party" in transactions. On the other hand, the Kyrgyz Republic's central location within the Eurasian continent, situated between the Western and Eastern economic zones, offers another advantage. This positioning can enhance its potential as a global integration hub by fostering a conducive legal environment for digitalization. These perspectives further support the notion of considering EU Law as a model for the Kyrgyz Republic.

[35] Theodora A. Christou – John L. Taylor: *Blueprint Paper on Digital Trade and the UNCITRAL Model Law on Electronic Transferable Records, 2023.* https://www.ebrd.com/documents/legal-reform/blueprint-paper-on-digital-trade.pdf.

Bibliography

Sandra Norman-Eady: Uniform Electronic Transaction Act. *Old Research Report,* 2000-R-1076. https://www.cga.ct.gov/2000/rpt/2000-R-1076.htm.

United Nations Economic Commission for Europe, Regulatory and Procedural Barriers to Trade in Kyrgyzstan Needs Assessment. United Nations, New York and Geneva, 2015. https://unece.org/DAM/trade/Publications/ECE_TRADE_412E-Kyrgyzstan.pdf.

Alba Zaragoza: eIDAS. The Digital Identification Regulation for Europe. The Signicat Blog, 17.07.2023, https://www.electronicid.eu/en/blog/post/eidas-regulation-electronic-signature/en.

Narmin Miriyeva: European Payments in the Digital Age. *ELTE Law Journal,* 2/2022.

Miklós Király: The Rise and Fall of Common European Sales Law. *ELTE Law Journal*, 2/2015.

Theodora A. Christou – John L. Taylor: *Blueprint Paper on Digital Trade and the UNCITRAL Model Law on Electronic Transferable Records, 2023.* https://www.ebrd.com/documents/legal-reform/blueprint-paper-on-digital-trade.pdf.

István Erdős: Private International Law in Business Transactions. Contracts Non-contractual obligations. Budapest, 2016 (https://edit.elte.hu/xmlui/handle/10831/30613).

THE ELECTRONIC IDENTIFICATION OF LEGAL PERSONS IN KYRGYZ REPUBLIC CAN HELP TO DEVELOP THE DIGITAL CONTRACTING

Dzhusupov Akylbek[1]

ABSZTRAKT ■ Tengerparttal nem rendelkező országként a Kirgiz Köztársaság kevésbé vesz részt a globális kereskedelemben. A világgazdaság digitalizálása azonban jó alkalom a lehetőségek kiegyenlítésére. Ebből a célból az olyan országok mint a Kirgiz Köztársaság, megfelelő jogi környezetet teremthetnek a jogi személyek elektronikus azonosításának fejlesztéséhez, és lehetővé tehetik a világ vállalatai számára, hogy kereskedjenek a régió országaival vagy szomszédaikkal (Kína, Oroszország). Az országnak különösen az európai és a világcégek számára ismert szabályokat kellene kialakítania. Ezért a fejlett országok legjobb jogi gyakorlatát a Kirgiz Köztársaság nemzeti jogszabályaiba is be kellene emelni.

ABSTRACT ■ As a landlocked country, the Kyrgyz Republic is less involved in global trade. However, the digitalization of the world economy is a good chance to equalize the opportunities. For this purpose, countries like the Kyrgyz Republic can create a legal environment for the development of electronic identification of legal persons and allow world businesses to trade with this region's countries or their neighbors (China, Russia). Especially, the country should establish the rules, which are familiar to European and world companies. Therefore, the best legal practices of developed countries should be introduced in the national legislation of the Kyrgyz Republic.

Kulcsszavak: digitalizálás, elektronikus azonosítás, jogi személyek, eIDAS, Kirgiz Köztársaság, EU

1. Introduction

Just like Hungary the Kyrgyz Republic (also known as Kyrgyzstan), is a landlocked country in the central part of the continent, with a population of more than 7,0 million people. It has borders with the People's Republic of China to the east,

[1] PhD student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

Kazakhstan to the north, Uzbekistan to the west and Tajikistan to the southwest. The territory is 199,951 square kilometers and most of it lies on large mountains. About 94% of the country rises over 1 000 m, and 40% at more than 3 000 m above sea level[2]. The som is the currency of Kyrgyz Republic (KGS), and its official languages are Kyrgyz and Russian.

2. General country information

On 31 August 1991, the Kyrgyz Republic declared its independence after the collapse of the USSR and started its own journey as a state. In my view, since that time the Kyrgyz Republic has been in search of its own brand of economic prosperity. Due to neighboring with the second largest economy in the world (China), a strong relationship with the biggest holder of natural resources (Russia), and landlocked highlands with cheap internet, we can concentrate on providing digital services for the commercial giants of the world. Especially to be a part of the huge trade between the European Union and China/Russia. The military conflict in the East of Europe started by Russia will have long-term negative effects on the direct relationship with two parts of the world. Apart from China and Russia the Kyrgyz Republic has the prospect of being a partner to communicate with economically fast-growing India.

Nowadays, the Kyrgyz Republic is a member of the following international and regional political and economic organizations:

1) Shanghai Cooperation Organization (SCO)[3] along with the Republic of India, the Republic of Kazakhstan, the People's Republic of China, the Islamic Republic of Pakistan, the Russian Federation, the Republic of Tajikistan and the Republic of Uzbekistan (The SCO focuses on cooperation with international and regional organizations);
2) Eurasian Economic Union (EAEU)[4] along with the Republic of Armenia, the Republic of Belarus and the Republic of Kazakhstan, the Russian Federation (The EAEU provides for free movement of goods, services, capital and labor, pursues coordinated, harmonized and single policy in the sectors determined by the Treaty and international agreements within the Union);

[2] National Investments Agency under the President of the Kyrgyz Republic, General information about Kyrgyz Republic, https://invest.gov.kg/about-kyrgyz-republic/general-information/.
[3] Shanghai Cooperation Organization, Member states of the SCO, https://eng.sectsco.org/20170109/192193.html.
[4] Eurasian Economic Union, Member states of the EAEU, https://eec.eaeunion.org/en/comission/about/.

3) Collective Security Treaty Organization[5] along with the Republic of Armenia, the Republic of Belarus, the Republic of Kazakhstan, the Russian Federation, and the Republic of Tajikistan, cooperate in the. (The objectives of the CSTO are the strengthening of peace, international and regional security and stability, the protection on a collective basis of the independence, territorial integrity and sovereignty of the member States);
4) Commonwealth of Independent States[6] (CIS) along with the Azerbaijan, the Republic of Armenia, the Republic of Belarus, the Republic of Kazakhstan, the Republic of Tajikistan, the Republic of Moldova, the Russian Federation, the Republic of Turkmenistan, the Republic of Uzbekistan and Ukraine, are the members of (According to the Charter of the CIS the objectives are the cooperation in political, economic, ecological, humanitarian, cultural and other field of development).

The Kyrgyz Republic is a member of more than 100 international organizations, including the OSCE, the Antiterrorist Center of the CIS Member States, the World Bank and others. In 2004, Kyrgyzstan became one of the founding states of the Eurasian group (EAG is an associate member of the Financial Action Task Force).

The Kyrgyz Republic has joined a number of treaties under which an interested party may address a claim to a court of the Kyrgyz Republic on recognition and enforcement of a decision issued by a court or arbitration court of another country[7]. The principal treaties are:

- UN Convention on Recognition and Enforcement of Foreign Arbitral Awards of 10 June 1958, joined by the Kyrgyz Republic in 1995;
- Convention on Legal Support and Legal Relations between the CIS Countries on Civil, Matrimonial, and Criminal cases of 22 January 1993, ratified by the Kyrgyz Republic in 1995.
- In 2004 the Kyrgyz Republic also ratified the Convention on Legal Support and Legal Relations on Civil, Matrimonial and Criminal Cases of 7 October 2002;

5 Collective Security Treaty Organization, The Charter of CSTO, https://en.odkb-csto.org/structure/#:~:text=In%20accordance%20with%20Article%203,sovereignty%20of%20the%20member%20states.

6 CIS, The historical information of the CIS in Russian language, https://e-cis.info/page/3509/80648/.

7 Kalikova & Associates, Business in the Kyrgyz Republic. Legal Aspects. The information and reference guide (2009). http://www.k-a.kg/sites/default/files/business_in_the_kyrgyz_republic_2009_eng.pdf.

- A number of bilateral agreements on mutual legal support with European Union, Azerbaijan, Iran, India, China, Latvia, Mongolia, Russia, Tajikistan, Turkey, Kazakhstan, United Arab Emirates, Uzbekistan, and other nations. In 2009, the Kyrgyz Republic recognized and enforced[8]:
- Decisions of other countries' arbitration courts established under the arbitration rules of the UN Commission for International Trade Law (UNCITRAL);
- Decisions of the courts of Armenia, Belarus, Kazakhstan, Latvia, Moldova, Russia, Tajikistan, Turkey, Turkmenistan, Ukraine, United Arab Emirates, and Uzbekistan on civil, matrimonial, and criminal cases;
  Decisions of the arbitration, economic and business courts of Azerbaijan, Moldova, Kazakhstan, Russia, and Tajikistan.However, now the Kyrgyz Republic recognizes and enforces the decisions of more countries, and this is a huge step towards legal and economic integration to the global market.

GDPs at PPP of Kyrgyzstan in 2009 – 14.7 bln, 2010 – 14.893 bln, 2011 – 16.106 bln, 2012 – 16.38 bln, 2013 – 18.439 bln, 2014 – 19.382 bln, 2015 – 20.58 bln, 2016 – 21.7 bln, 2017 – 23.15 bln, 2018 – 24.54 bln, 2019 – 26.08 bln, 2022 - 22.2 bln. Financial institutions include mortgage companies (organizations), commercial banks, credit unions, leasing companies (organizations), pawnshops, microfinance organizations (microcredit agencies, microcredit companies, microfinance companies, specialized financial institutions), savings pension funds, exchange bureaus, operators of e-money payment systems, reinsurance organizations and brokers, payment organizations, postal service enterprises, professional participants of the securities market, building and loan associations, insurance organizations (insurers), insurance brokers, commodity exchanges, e-money issuers and agents (distributors) of electronic money[9].

According to the National Development programme of the Kyrgyz Republic until 2026 the Government is planning to attract investment to create national digital infrastructure, which should be able to support new demands of digital relationship. The national digital infrastructure will include networks, data centers, cloud technologies, information and service access centers, digital platforms, including broadband and broadcasting. The digital infrastructure must be able to support the rapid growth of traffic, provide coverage with sufficient

[8] Ibid.

[9] The Eurasian group on combating money laundering and financing of terrorism (EAG) is a FATF-style regional body: Information on Kyrgyz Republic https://eurasiangroup.org/en/kyrgyzskaya-respublika.

bandwidth to meet new needs[10]. In this regard, it should be essential to develop different forms of electronic identification of persons which are expected to be a participant of all business relationships. The electronic identification of natural persons is quite developed in Kyrgyz Republic and now it is time to create an environment for online identification of legal persons as well.

2.1. The concept of digitalization of the Kyrgyz Republic

The main obstacles to the investment climate in the Kyrgyz Republic include poor infrastructure, political instability and a small market size. The European Bank for Reconstruction and Development highlights the market size as a critical issue, and I agree with their conclusion. The Kyrgyz Republic should focus on attracting investment and offering services to economically developed countries like China and Russia. I believe that in the near future the war in Ukraine will stop and the world will restore global trade with Russia. Then, buying natural resources from Russia will again be a good deal both for buyers and sellers. Additionally, serving as a retail trading platform for European consumers purchasing goods from China is a viable option. Digital contracting and electronic identification of legal entities are key strategies for landlocked countries to integrate into the global market and offer a unique instrument for communication. In the Kyrgyz Republic, digital contracting has the potential to play a significant role in the country's economic development. By enabling businesses to enter into contracts more efficiently and securely, digital contracting can reduce transaction costs and facilitate trade and investment. This, in turn, can lead to increased productivity, job creation and economic growth.

However, in order to develop digital contracting the Kyrgyz Republic must establish a new law on electronic identification of legal persons. The new rules will eliminate the sidesteps situations, in which legal persons give up due to a complex process and the need to verify themselves in a commercial office, store or branch of the company they want to become clients or partners of, and, on the other hand, give the government the necessary tools to improve their digital

[10] The National development programme of the Kyrgyz Republic until 2026: Article 4.2., paragraph 2. http://cbd.minjust.gov.kg/act/view/ru-ru/430700. Original text as follows: *"Uluttuk sanariptik infratüzümgö tarmaktar, maalymattardy ishtep chyguu borborloru, bulut tekhnologii, maalymattarga zhana kyzmat körsötüüülörgö zhetüü borborloru, sanariptilar, anyn ichinen keñiri tilkellu ü baylanysh zhana radio berüü kiret. Sanariptik infratüzüm trafiktin tez ösüshün karmap turuuga, zhañy kerektöölördü kanaattandyruu üchün zhetishtüü ötkörüü zhöndömdüülügü menen kamsyz kyluuga zhöndö mdüü abalda boluuga tiyish".*

processes in favor of the companies, creating better and smoother relationships, reducing waiting, workload, and, overall, frustration. The electronic identification will help to enhance utilizing the electronic signature for the business entities.

Moreover, the pandemic in 2020 highlighted the importance of electronic identification in enabling businesses to operate remotely and maintain continuity in times of crisis. The Kyrgyz Republic has already revealed a strong trend in digitalising its government, as captured by the e-Government Development Index, which measures the readiness and capacity of national institutions to use ICTs to provide public services[11]. Kyrgyzstan was ranked amongst the top 10 reforming countries in 2018, along with Uzbekistan and Kazakhstan. This upward trend was largely carried by a higher e-participation index, with enhanced access to information and increased citizen's involvement in the decision making process. Electronic identification and digital signature can help businesses in the Kyrgyz Republic to adapt to the new normal and continue to operate in a safe and efficient manner.

The idea of the new Law on electronic identification of legal persons in the Kyrgyz Republic is to create a certain legal environment, where legal persons could be identified by the private or governmental digital platforms and verified by state authorities which have the database of all legal persons. After electronic identification all legal entities could join any relationship through utilizing the electronic signatures.

2.2. Comparing and contrasting the Kyrgyz Republic's legal framework with the existing legal framework in the EU

In my previous research I have identified the following similarities and differences in legal frameworks of the Kyrgyz Republic and European Union. Let me start with similarities which are common for both of them:

1) Recognition of electronic means of concluding a contract;
2) Electronic commerce is legally allowed on their territories;
3) Electronic signature is available both for natural or legal persons;
4) Personal data is a vital part in digital contracting;

[11] OECD, Supporting Firm Creation and Growth through Business Development Services in Kyrgyzstan, Paris, 2020. https://www.oecd.org/eurasia/competitiveness-programme/central-asia/Supporting-Firm-Creation-and-Growth-through-Business-Development-Services-in-Kyrgyzstan-ENG.pdf.

There are also differences between the Kyrgyz Republic and the European Union. They are as follows:

1) Contrary to the European Union, the electronic seal and electronic time stamp are not introduced as a separate business tool to the national legislation of the Kyrgyz Republic. However, the using of enhanced electronic signature on the territory of the Kyrgyz Republic includes the seal of the legal entity;
2) The national legislation of the Kyrgyz Republic does not provide standardized contracts for digital relationships. However, the EU Law has certain provisions for digital content and services, as well as for digital sales of goods.
3) In contrast to EU Law, the Kyrgyz Republic's legislation does not allow parties to choose as governing law the non-state law. According to Article 1198(1) of Civil Code of the Kyrgyz Republic: *"The contract is governed by the law of the country chosen by agreement of the parties, unless otherwise provided by law"*[12]. However, pursuant to Rome-I regulation, parties can identify a non-state law or international convention in their contracts.
4) European Union Law allows the electronic identification of legal persons, however the Kyrgyz Republic doesn't guarantee the same permission.

In this article I would like to research the legal possibility of electronic identification of the legal persons in the Kyrgyz Republic and what we can do to boost it. Especially, if businesses can start providing their services on a remote base for legal persons without concluding contracts on hard copies. Of course, as usual, I would like to use EU Law as a model law.

2.3. Identifying potential legal reforms or amendments

First, in order to be competitive with the world countries and attract investors or customers to purchase through Kyrgyz platforms, the legislators of the country should develop the system of identification of all business participants. This system should allow to identify foreign citizens and legal entities registered in Kyrgyz Republic (at first stage), and all legal persons at next stages.

Second, currently the Kyrgyz Republic, as well as other Central Asian countries, does not permit accepting trust services of other states, including those of neighboring countries. There is also no permission for that within the

[12] The original version of Civil Code of the Kyrgyz Republic as of 05.01.1998 #1, http://cbd.minjust.gov.kg/act/view/ru-ru/5?cl=ru-ru.

framework of the economic integration organization. The Shanghai Cooperation Organization nor Eurasian Economic Union did not adopt a legal act recognizing the trust services, including electronic signatures of partner countries. However, in order to contribute to their general cross-border use, the European Union made it possible to use trust services as an evidence in legal proceedings in all Member States.[13] Therefore, the qualified electronic signature, qualified electronic seal and qualified electronic time stamp issued in one EU Member State shall be recognized as a qualified electronic time stamp in all Member States (Articles 25(3), 35(3), 41(3)).

From 2015 there is a strong recommendation from the UNECE on promoting a wider use of electronic documents by traders. Particularly, they ask to ensure the implementation of the law "On Electronic Document and Digital Signature"[14]. Immediate steps, as suggested by some State officials, include amending the laws governing the procedures and activities of individual State agencies, with a view to provide clear guidelines for implementing digital signatures. State agencies should also receive advanced training in this area, and equipped with the required tools and management information systems to ensure data storage security[15]. Therefore, the legal reforms must be directed to provide easy use of electronic signatures in every sphere of the business and none-business as well.

For the European authorities the objective was to establish a digital single market by 2015, focusing on key aspects of the digital economy and promoting seamless cross-border utilization of online services. Special emphasis is placed on facilitating secure electronic identification and authentication to achieve a fully integrated digital single market[16]. Therefore, the same goal should be achieved also by the Central Asian countries, including the Kyrgyz Republic.

2.4. The essential findings and arguments of the previous research

One of the reasons for barriers to trade in the Kyrgyz Republic is lack of using electronic tools. Therefore, even in the report of the United Nations Economic Commissions for Europe seven years ago there was the following recommendation:

[13] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, 73-114.

[14] This Law was abolished after the adoption of the Law on Electronic Signature.

[15] United Nations Economic Commission for Europe, Regulatory and Procedural Barriers to Trade in Kyrgyzstan Needs Assessment (21).

[16] eIDAS Regulation, 73–114.

"Ensure the implementation of the law "On Electronic Document and Digital Signature". Immediate steps, as suggested by some State officials, include amending the laws governing the procedures and activities of individual State agencies, with a view to provide clear guidelines for implementing digital signatures. State agencies should also receive advanced training in this area, and equipped with the required tools and management information systems to ensure data storage security"[17].

In most European cases before 2014, citizens of one Member State could not use their electronic identification to authenticate themselves in another Member State, because the national electronic identification schemes in their country are not recognized in other Member States. That electronic barrier excluded service providers from enjoying the full benefits of the internal market. Therefore, the lawmakers of Kyrgyz Republic should allow the use of electronic identification of legal persons and foreign citizens. Mutually recognized electronic identification means will facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities.

One of the challenges is lack of the legal base for providing proofs. The court of the Kyrgyz Republic still accepts paper-based proofs during the cases. They do not accept electronic files because their trial case files include only documents in paper format. At the same time, the parties cannot just print necessary documents by using a stamp. Therefore, it is essential to develop the civil procedural legislation including certain regulations on collecting files not only in paper-based format, but in electronic way too.

Another important part of the contacts is payment issues. In that regard, European authorities pay high attention to the electronic payment (e-payment), which is a process of paying for transactions without using cash by using an e-payment system or medium instead. It is too hard to imagine that someone will use cash during the concluding of a contract through electronic means. The use of e-payment has expanded as the use of internet-based banking and e-commerce has grown. In modest international commercial transactions, e-payment frequently replaces using a credit or debit card[18].

I would like to notice that not all legal introductions will have success. New digital rules should be accepted by the market, and especially by the big tech players around the world, particularly by European ones. In his article "The Rise and Fall of Common European Sales Law", Miklós Király, Head of Department and Professor of Private International Law and European Economic Law and

[17] United Nations Economic Commission for Europe, Regulatory and Procedural Barriers to Trade in Kyrgyzstan Needs Assessment (21).

[18] Narmin Miriyeva: European Payments in the Digital Age. *ELTE Law Journal,* 2/2022.

former Dean of ELTE University Faculty of Law, Member of Expert Group on a Common Frame of Reference in the area of European Contract Law shared with his predictions. *"Despite all these uncertainties, one day the project of European contract law may come back to the legislative agenda. The idea is not completely forgotten; the CESL remains one of the reference texts for European contract law. The forty year long history of the preparation of the Statute of the European Company (SE), which quite suddenly brought results, may console those who supported and still support the development of CESL. However, in order to achieve this goal, political and institutional support and clear and visionary guidance are needed. The fate of European contract law depends on the institutional dynamics and future of the EU, too"*[19].

So, it is feasible to develop a new law on electronic identification of legal persons based on the eIDAS regulation in the Kyrgyz Republic, with necessary amendments to suit the local context. If there are concerns about potential risks for the parties involved, the use of the new law can be optional. Parties and entities would have the discretion to activate their rights and assume responsibility accordingly. Nonetheless, it is essential to provide them with advanced electronic tools to facilitate business relationships electronically.

3. Legal analysis of the different laws

3.1. A comprehensive legal analysis of Kyrgyz Law

Electronic signature. The Civil code of KR provides a regulation on enforcing a contract which is signed by the electronic signature. Pursuant to Art. 176 (2): *"A facsimile reproduction of a signature by means of mechanical or other copying, electronic signature or any other analogue of a personal signature is permitted if provided for by law or by agreement of the parties".*

The electronic signature is vital for electronic identification because we could not even imagine applying for something or concluding a contract without using the remote tools of acknowledging the issue by the parties. In paper-based documents you usually use the handwritten signature, so in digital documents you can use the electronic signature. The Law of the Kyrgyz Republic on Electronic Signature № 128 as of July 19, 2017 (Law on Electronic Signature) governs the relations on use of digital signatures when making civil transactions, rendering the state and municipal services, execution of the state and municipal functions, and also when making legally significant actions.

[19] Miklós Király: The Rise and Fall of Common European Sales Law. *ELTE Law Journal*, 2/2015.

As it described in Article 2 of the Law on Electronic Signature *the digital (electronic) signature (ES) - information electronically which is attached to other information electronically and (or) is logically connected with it and which is used for determination of person on behalf of which information is signed*[20].

This Law allows the usage of two types of electronic signature:

1) Simple electronic signature;
2) Enhanced electronic signature (qualified, unqualified).

In accordance with the Law on Electronic signature natural persons are entitled to use the simple ES, because it can be presented in form of codes, chiffres and this is equal to signing a document in a handwritten form. On the other hand, the enhanced ES is equal to signing a document in a handwritten form and putting a seal on it. Therefore, this kind of electronic signature is more suitable for legal entities.

The usage of the electronic signature for natural persons is widespread in Kyrgyz Republic and most of the business sectors have been providing services since the end of the pandemic. However, for legal persons there are still a lot of challenges.

On the "Law" level we have less opportunities for electronic identification of persons. However, the next level of lower legal acts includes appropriate acts, which establish the rules for remote legal relationships. For instance, law-making bodies like the Cabinet of Ministers and National Bank of the Kyrgyz Republic issued decrees addressed to welcome the usage of electronic signatures and provide online services. The Decree of the Cabinet of Ministers "On approval of the Procedure for state registration (re-registration) and registration of termination of activities of legal entities, branches (representative offices) in electronic form"[21] allows the identification of legal persons (including foreign ones) while signing a certain decision for opening a company. Also, the National Bank issued a Decree "On the Procedure for Identification and Verification of Clients Remotely"[22]. This Procedure allows banks to provide services and products through online platforms or mobile applications, but only for natural persons - citizens of the Kyrgyz Republic.

[20] The unofficial translation of the Law of the Kyrgyz Republic on Electronic Signature № 128 as of July 19, 2017 https://cis-legislation.com/document.fwx?rgn=99019.

[21] The Cabinet of Ministers of the Kyrgyz Republic, Decree "On approval of the Procedure for state registration (re-registration) and registration of termination of activities of legal entities, branches (representative offices) in electronic form", https://cbd.minjust.gov.kg/7-23622/edition/3067/ru.

[22] The National Bank of the Kyrgyz Republic, Decree "On the Procedure for Identification and Verification of Clients Remotely", https://nbkr.kg/contout.jsp?item=103&lang=RUS&material=106190.

3.2. A comprehensive legal analysis of EU laws and regulations

The European Parliament and the Council of the European Union have adopted the Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC[23] (eIDAS Regulation), which establishes a framework for electronic identification and trust services for electronic transactions in the internal market. According to Article 1, the eIDAS Regulation:

a) lays down the conditions under which Member States recognize electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;

b) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

The essential element for enforceability of the contract is identification of the parties which are going to be Parties. According to eIDAS Regulation: The objective is to bolster confidence in electronic transactions within the internal market. It aims to establish a shared basis for secure electronic interactions among citizens, businesses, and public authorities. This, in turn, will enhance the efficiency of both public and private online services, electronic business, and electronic commerce across the European Union. However, this Regulation does not affect national, or EU law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form.

The eIDAS certification sets the standards and criteria for simple electronic signature, advanced electronic signature, qualified electronic signature, qualified certificates and online trust services. Furthermore, it rules electronic transactions and their management[24]. However, what we need the most from this Regulation is that it has essential principles for identification of legal persons. Particularly, it says that "electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person". So, European legislators suggest that every legal entity might be identified through a natural person (for instance Chief Executive Officer or Authorized Lawyer).

[23] eIDAS Regulation, 73-114.

[24] Alba Zaragoza: eIDAS. The Digital Identification Regulation for Europe. The Signicat Blog, 17.07.2023, https://www.electronicid.eu/en/blog/post/eidas-regulation-electronic-signature/en.

3.3. Legal analysis of US laws and regulations

In the United States, the Uniform Electronic Transactions Act (UETA)[25] and the Electronic Signatures in Global and National Commerce Act (ESIGN)[26] define and govern digital interactions.

The ESIGN does not explicitly address the identification of legal persons. Its primary focus is on ensuring that electronic signatures are treated as equivalent to handwritten signatures for the purposes of federal law.

While ESIGN doesn't directly regulate the identification of legal persons, it does have provisions that could indirectly impact this area:

- Electronic Signatures: The Act defines electronic signatures and establishes their legal validity. This can be relevant to the identification of legal persons in certain contexts, as electronic signatures can be used to authenticate and verify the identity of parties to a transaction.
- Electronic Records: ESIGN also provides a legal framework for electronic records, which can be used to document the identity and actions of parties involved in a transaction.

The UETA primarily focuses on facilitating electronic transactions and signatures, but it also does not explicitly address the identification of legal persons in a detailed manner like the e-IDAS Regulation does. UETA establishes the validity of electronic records and signatures in business transactions, but it treats parties in general without specifying distinct regulations for legal persons versus natural persons.

UETA provides uniform rules governing electronic commerce transactions. It sets a legal foundation for the use of electronic communications in business transactions where the parties have agreed to deal electronically. UETA validates and supports the use of electronic communications and records and places electronic commerce and paper-based commerce on the same legal footing. According to UETA, the term "Electronic" has the same meaning as in ESIGN[27]. Therefore, we can consider that a digital contract is "an agreement created and

[25] Federal Deposit Insurance Corporation FDIC, *Consumer Compliance Examination Manual,* January 2014. https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/10/x-3-1.pdf.

[26] Section 106, ESIGN.

[27] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf.

signed by electronic means". The act is designed to facilitate and promote commerce and governmental transactions by validating and authorizing the use of electronic records and signatures and to promote uniform electronic transaction laws among the states. It is also designed to be consistent with other applicable laws[28].

3.4. Legal analysis of international laws and regulations

One of the fundamental laws for all countries including the Kyrgyz Republic and Member states of the European Union is certainly the Model Law of the United Nations Commission on International Trade Law (UNCITRAL).

It started in 1996 with adoption of the Model Law on Electronic Commerce (MLEC)[29] by UNCITRAL. These rules are designed to eliminate legal barriers and enhance legal predictability in electronic commerce transactions. One of the main goals of the MLEC is to tackle challenges posed by legal requirements that cannot be modified by contracts. By ensuring equal treatment for both paper and electronic information, the MLEC encourages paperless communication, enhancing efficiency in global trade. It establishes a unified legal framework that supports electronic commerce and fosters harmonization across different legal systems.

Then on 5 July 2001 UNCITRAL adopted the Model Law on Electronic Signatures (MLES)[30]. The increasing reliance on electronic authentication methods, replacing traditional handwritten signatures, has underscored the need for a legal framework addressing their use. The Model Law on Electronic Signatures (MLES) builds on the principles of the MLEC, ensuring that electronic signatures fulfill their legal function in a technology-neutral way. By not favoring any specific technology, such as cryptographic digital signatures, the MLES enables various types of electronic signatures to be legally recognized. This adaptability promotes flexibility in authentication methods within the legal framework.

[28] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf.

[29] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Transferable Records, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf.

[30] United Nations Commission on International Trade Law, UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mlit_advance_copy.pdf.

Therefore, the aim of the MLES was to enable and facilitate the use of electronic signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures. Thus, the MLES may assist States in establishing a modern, harmonized and fair legislative framework to address effectively the legal treatment of electronic signatures and give certainty to their status.

The MLES is founded on the core principles found in all UNCITRAL texts related to electronic commerce: non-discrimination, technological neutrality, and functional equivalence. It defines criteria to assess the reliability needed to equate electronic signatures with handwritten ones. The MLES also outlines key rules of conduct for signatories, relying parties, and trusted third parties. Additionally, it promotes the recognition of foreign certificates and electronic signatures, following substantial equivalence, thereby facilitating cross-border transactions and enhancing international cooperation on electronic signature validity.

After that in 2017 UNCITRAL decided to adopt Model Law on Electronic Transferable Records (MLETR)[31]. This step was taken to facilitate the legal use of electronic transferable records domestically and internationally. The MLETR applies to electronic transferable records that offer functional equivalence to paper-based transferable documents or instruments. These include documents that give the holder the right to claim performance of an obligation and allow a transfer by changing possession of the document. Common examples include bills of lading, bills of exchange, promissory notes and warehouse receipts. The framework supports the legal recognition and usage of these instruments in an electronic form.

Finally, on 7 July 2022 UNCITRAL adopted the Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT)[32]. This law aims to establish a unified legal framework that supports the use of identity management services for the online identification of individuals and legal entities. It also governs the use of trust services to guarantee the integrity and reliability of electronic data. Furthermore, the MLIT introduces mechanisms to promote the cross-border recognition of both identity management and trust services, ensuring seamless electronic interactions across different jurisdictions.

[31] United Nations Convention on Contracts for the International Sale of Goods, New York, 2010, (31). https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-09951_e_ebook.pdf.

[32] The unofficial translation of the Civil code of the Kyrgyz Republic: https://www.libertas-institut.com/de/Mittel-Osteuropa/Civil%20Code%20part%20I.pdf.

Digital trade relies on trust in the identities of business partners and the accuracy of electronic data exchanged. The MLIT sets a uniform legislative standard to promote trust in digital transactions and documents. As the first global legislative text of its kind, it serves as a legal foundation for digital trade worldwide, complementing other UNCITRAL legislative texts related to electronic commerce.

The first part defines relevant terms, outlines the scope of application, and establishes general provisions regarding the voluntary use of identity management and trust services, as well as their relationship with other laws.

The second part establishes the fundamental elements of the legal framework applicable to identity management. It outlines core obligations for identity management service providers and subscribers, and sets rules regarding the liability of identity management service providers. Notably, Article 9 introduces a key provision on functional equivalence, which states that offline identification and identification conducted through identity management must be functionally equivalent and rely on a reliable method. The reliability of the method is assessed either retrospectively based on the circumstances or prospectively through designation.

The third part establishes the foundational elements of the legal framework for trust services, including provisions regarding the liability of trust service providers. Articles 16 to 21 specify the functions of certain trust services (e.g., electronic signatures, electronic seals, electronic timestamps, electronic archiving, electronic registered delivery services, and website authentication) and the associated requirements. Similar to identity management, the reliability of the method used for trust services is assessed retrospectively based on the circumstances outlined in Article 22 or prospectively through designation as per Article 23.

The fourth part focuses on enabling the cross-border recognition of identity management and trust services, a key objective of the Model Law. It employs a decentralized approach and utilizes both retrospective and prospective mechanisms for assessing the reliability of the methods employed.

Since the MLIT sets rules for identity management services which ensure the online verification of individuals and legal entities and trust services confirm the authenticity and reliability of digital data. These essential services are generally provided by specialized third-party entities, fostering secure transactions and safeguarding the integrity of digital interactions. Therefore, these UNCITRAL standards should also, along with e-IDAS regulation, be the Model law for the Kyrgyz Republic in establishing a legal environment for legal persons' identification.

4. A new law on electronic identification of legal persons

The existing legislation of the Kyrgyz Republic provides all opportunities to use electronic signature in business relationships. However, it is hard to implement it, because trust services are undeveloped in the country. There is no big company that can issue technological tools for wider usage of the electronic signature for the majority of legal persons. Moreover, businesses accepting the electronic signatures should have a relationship with the same trust services as their counterparties. Therefore, the digitalization of legal persons is a bit challenging in the Kyrgyz Republic. On the contrary, the usage of the electronic signatures among individuals became a "hot topic" for various sectors, since codes and passwords inserted by a natural person upon receiving SMS or push-notifications to their phone are considered as one type of using electronic signatures.

In this regard, I would like to suggest researching the cheapest way of increasing the electronic identification through legal means of some institutions. For instance, there is no creation of nature such as "legal person", it is a result of human thinking after the development of the economy. However, every legal person is associated with certain individuals. They are founders, managers and employees. The same opinion was formulated in the research of Michael Sonntag from Johannes Kepler University: *"There is always the need for a natural person to act for them (legal persons), although the results of them are ascribed to the legal person. The same is true even when the company acts through machines: There is always a natural person, who installed and set up the machine"*[33].

Therefore, we should create a system of identification of legal persons through natural persons who can act on behalf of them. According to Kyrgyz legislation and international rules the head of the executive body of the company is usually an authorized person (CEO, President, Chairman of the Board, Boss), but this person should be responsible to sign on behalf of the legal person. Therefore, we should identify an entity by electronic means through its manager. In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers.

Therefore, I believe that the contract signed with an electronic signature designed for natural persons still can be valid. I was inspired by the opinion of Jos Dumortier, Professor of Law – K.U.Leuven. He wrote: *"It is a common*

[33] Michael Sonntag: Electronic Signatures for Legal Persons. In: Susanne Hofer – Manfred Beneder (ed.): *IDIMT-2000. 8th Interdisciplinary Information Management Talks, Proceedings.* Linz, Universitätsverlag Rudolf Trauner, 2000.

misunderstanding that, in Europe, in order to have a legally valid electronic signature, you need a "qualified" electronic signature"[34]. The understanding that in Kyrgyz Republic the usage of only "qualified electronic signature" for legal persons should be accepted as incorrect.

As an alternative way, the Ministry of Justice of the Kyrgyz Republic as a state department for registering legal entities might create a strong information and technology platform, which will contain all data on legal persons. Especially, online updating information about the managers of the company with their sample of signatures. There is already a platform in the Kyrgyz Republic under control of this Ministry, however, it contains mostly data from the initial registration. There is no strict requirement of the notification of the replacement of the management board. Still, the majority of the companies have not been updating their managerial information. But the biggest current problem is that the specimen of the manager's signature is not available, therefore nobody knows how to identify the authorized persons of the legal entities.

This kind of approach has already been created in Hungary, where you can be identified as a legal person just providing information from the database. For instance, banks can open bank accounts using the documents and check the signature from that system. Companies do not need to provide a notarized specimen of signature of their authorized persons as required in the Kyrgyz Republic's bank legislation. It is too challenging if one company wants to open an account in several banks, because they have to verify the specimen of signatures for each of them by a notary. Additionally, in Hungary the contract signed by the manager without putting a stamp is still valid.

5. Conclusion

Benefits of Electronic Identification for Digital Contracting in the Kyrgyz Republic.

- Electronic identification can streamline the process of verifying the identity of legal persons, reducing paperwork and administrative costs. This can make digital contracting more efficient and attractive to businesses.
- A robust electronic identification system can enhance the security of digital contracts by reducing the risk of fraud and identity theft. This can foster trust among parties involved in online transactions.

[34] J. Dumortier: Legal Status of Qualified Electronic Signatures in Europe. In: S. Paulus – N. Pohlmann – H. Reimer (ed.): *ISSE 2004 – Securing Electronic Business Processes. Highlights of the Information Security Solutions Europe 2004 Conference*. Wiesbaden, Vieweg+Teubner Verlag, 2004. 281-289. ,

– By establishing clear legal frameworks and standards for electronic identification, Kyrgyzstan can provide greater legal certainty for digital contracts. This can encourage businesses to adopt digital technologies and participate in the digital economy.
– Aligning Kyrgyzstan's electronic identification laws with international standards can facilitate cross-border digital transactions and promote economic integration.

By studying and adapting above mentioned European and International laws and standards, the Kyrgyz Republic can create a legal environment that supports the development of digital contracting and promotes economic growth.

Bibliography

Miklós Király: The Rise and Fall of Common European Sales Law. *ELTE Law Journal*, 2/2015.

Michael Sonntag: Electronic Signatures for Legal Persons. In: Susanne Hofer – Manfred Beneder (ed.): *IDIMT-2000. 8th Interdisciplinary Information Management Talks, Proceedings.* Linz, Universitätsverlag Rudolf Trauner, 2000.

J. Dumortier: Legal Status of Qualified Electronic Signatures in Europe. In: S. Paulus – N. Pohlmann – H. Reimer (ed.): *ISSE 2004 – Securing Electronic Business Processes. Highlights of the Information Security Solutions Europe 2004 Conference*. Wiesbaden, Vieweg+Teubner Verlag, 2004. 281-289.

Narmin Miriyeva: European Payments in the Digital Age. *ELTE Law Journal,* 2/2022.

Alba Zaragoza: eIDAS. The Digital Identification Regulation for Europe. The Signicat Blog, 17.07.2023, https://www.electronicid.eu/en/blog/post/eidas-regulation-electronic-signature/en.

Kalikova & Associates, Business in the Kyrgyz Republic. Legal Aspects. The information and reference guide (2009). http://www.k-a.kg/sites/default/files/business_in_the_kyrgyz_republic_2009_eng.pdf.

United Nations Economic Commission for Europe, Regulatory and Procedural Barriers to Trade in Kyrgyzstan Needs Assessment. United Nations, New York and Geneva, 2015. https://unece.org/DAM/trade/Publications/ECE_TRADE_412E-Kyrgyzstan.pdf

CAN FINES STIMULATE PUBLIC CONTROL ON LEGISLATION?

Ákos Kántor[1]

ABSZTRAKT ■ A jogalkotás szabályainak viszonylagos állandósága a demokrácia záloga, mivel a jogszabály egyik érvényességi kelléke, hogy szabályozott keretek között szülessen meg, melyre nézve kifejezetten hátrányosan hat a gyakori változás.
A jogalkotásra vonatkozó szabályok korábban szankciót nem tartalmazó, *lex imperfecta* jellegűnek voltak mondhatók, mivel csak a legkomolyabb normasértések okozták a jogszabállyal szemben alkalmazható legsúlyosabb szankciót: a közjogi érvénytelenséget, melynek megállapítása hosszadalmas folyamat.
A 2022-ben történt törvénymódosítással olyan módon változott meg a jogalkotási eljárás, amely a jogszabályelőkészítésben való társadalmi részvétel elmulasztását pönalizálja. Az eljárás is rendhagyó, mivel a kormányzati ellenőrzési szerv évente vizsgálja a kötelezettség teljesítését, és a mulasztó szervezetre jelentős mértékű bírságot ró ki.
A kormányzati jogalkotási tevékenység vizsgálatáról éves jelentés készül az Európai Unió részére, amelyre az EU a következő éves jogállamisági jelentésben reagál.
Jelen tanulmány célja a hazai jogalkotási eljárás változásai és az első vizsgálati ciklus tapasztalatai, az arról készült vizsgálati (KEHI) jelentés, valamint az EU visszajelzésének bemutatása. Az előzményekben a vonatkozó szakirodalmi elméletek kerülnek áttekintésre, különös tekintettel a jogalkotási folyamat hiányainak hatásaira. A változások és a vizsgálat megállapításainak ismertetése magyarázattal szolgál arra nézve, hogy a jogszabályok *lex imperfecta* jellege hogyan és miért látszik megszűnni.

ABSTRACT ■ The key of democracy is the relative stability of the rules governing legislation, given that one of the conditions for a law to be valid is that it shall be adopted within a regulated framework—a particularity that is negatively affected by frequent changes.
The rules on legislation were previously lex imperfecta, lacking sanction, since only the most serious breaches of law triggered the application of the gravest sanction against the law, namely public-law invalidity, which takes a lengthy process to establish.
With the legislative amendment in 2022, the legislative procedure has been altered so that the absence of public participation should be penalised. The procedure itself is also unusual: the Government's controlling body examines each year the fulfilment of the obligations, and imposes substantial fines on organisations in default.

[1] PhD student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

An annual report is prepared for the European Union regarding the rule of law, to which the EU reacts in its next annual Rule of Law Report.
My study aims to describe the changes in the Hungarian legislative procedure and the experience gained in the first cycle of examination, and to present the corresponding report prepared by the Hungarian Government Control Office (hereinafter: KEHI) and the EU's assessment of the same. It will also review relevant theories presented in literature, especially those concerning the impacts of the shortcomings of the legislative procedure. Presenting the changes and findings of the assessment will explain how and why the lex imperfecta nature of the legislation seems to be diminishing.

Keywords: legislation, public participation, lex imperfecta, Hungarian Government Control Office, KEHI investigation, fines

1. History

The rules governing legislation are characterised by relative permanence, despite the fact that an important feature of law is its variability[2]. Yet, the regulation of legislation varies rhythmically, with Act XI of 1987 on law-making being followed only 23 years later by Act CXXX of 2010[3] of the same title, which, after numerous amendments, is still in force today.

The provisions regulating the legislative process are lex imperfecta[4], since only a very serious breach of these grants means the application of the only possible sanction, i.e. invalidity under public law.

An important requirement for a law to be valid is that it must have been drafted in accordance with the legal norms in force at the time. This requirement also makes it important to preserve the relative stability of the system of rules governing legislation[5]. The Constitutional Court of Hungary has also pointed

2 Cp. Zoltán Tóth J.: *Jogalkotástan Jogdogmatikai és jogszabályszerkesztési ismeretek*. Budapest, Dialóg Campus Kiadó, 2019. 37.

3 The fundamental difference between the two laws is that while the 1987 law required a two-thirds vote of the members present to pass, the 2010 law is not considered a cardinal law. The old Jat. was also amended several times, but between 17.01.2001 and 15.06.2007 – for six years – the text did not change, which may be due to the need for a qualified majority amendment.

4 *„Vannak jogtételek, melyek a bennök foglalt parancs megszegéséhez semminemű szankciót (másodtételt) nem fűznek (leges imperfectae)"* Gusztáv Szászy-Schwarz: *Parerga – Vegyes jogi dolgozatok*. Budapest, Athenaeum Irodalmi és nyomdai részvénytársulat, 1912. 14.

5 For example, the text of the Jet. remained unchanged for almost six years between 01.08.2013 and 14.04.2019, while the longest such period for the Jat. was four year long, between 06.06.2014 and 17.05.2018.

out in several decisions that the procedural guarantees of legislation derive from the rule of law principles and those of legal certainty; therefore a valid law can only be created by observing the rules of formalised procedure. This is a formal requirement and therefore relatively easy to assess for those who have a view of the whole legislative process. The purpose of defining formal validity criteria is to reduce legal uncertainty as to whether a given provision constitutes a legal norm and is therefore legally binding.

The Constitutional Court has a consistent history of examining the observance of the rules of legislative procedure guaranteeing the observance of the rules of the legislative procedure and can thus annul a law adopted in a legislative procedure that is seriously flawed in its form. In the case of Acts, serious formal defects imply errors in the parliamentary procedure. In the preparatory phase of a law, a failure to consult the public as required by law or to carry out a prior impact assessment may constitute a formal defect. However, according to the consistent practice of the Constitutional Court, the mere procedural omission by the legislator to obtain the views of the persons concerned from the bodies entitled under the legislative law during the preparatory stage of the legislative process does not, as a general rule, render the legislation unconstitutional, unless a specific and institutionalised obligation to provide an opinion is provided for in a separate law.

The Hungarian Parliament introduced the publicity of legislation with Act CXXXI of 2010 to promote, as part of good governance, the involvement the most diverse groups of society in the preparation of laws, thereby enabling a multifaceted grounding of legislation in the public interest and thus improving the quality and enforceability of laws[6]. Public participation in the legislative process is achieved through various forms of consultation rights. These include, in particular, the right to comment, the right to be informed, the right to make proposals and the right to express an opinion.[7] Ildikó Vadál stated that information is an indispensable condition for public participation in the legislative process, but in order for an informed opinion to be made, it is necessary to have access to other materials in addition to the draft norm, such as impact assessments and expert materials. It is important that sufficient time is allowed for consultation, but in practice the legislative departments have often failed to ensure this, often claiming that they too had less than the required five days. Vadál herself highlighted the shortcomings of the legislation, which does not penalise failure

[6] Cp. István Stumpf: Az Alkotmánybíróság és az Országgyűlés viszonya a közjogi érvénytelenség tükrében. *Miskolci Jogi Szemle*, 2020/1, 277–290. 277-278.

[7] Cp. Ildikó Vadál: *A kormányzati döntések konzultációs mechanizmusai.* Budapest, CompLex, 2011. 101.

to carry out the social consultation process or to do so properly. In her book, she proposed clarifying the rules and adding guarantee rules. She argued that a guarantee element would be to provide a legal remedy in the event of a breach of the rules on the consultation procedure by public bodies[8]. A similar conclusion was reached by the drafters of the document entitled Társadalmi Egyeztetés Eljárási Normarendszere[9], who proposed a system of sanctions for infringements of the rules on public access to legislation, which would not establish political responsibility and consequences[10]. In the case of a serious breach, they proposed the annulment of the legal norm adopted.

The relative stability expected from legislation based on democratic requirements was affected by many other factors besides the accelerated development in recent years, such as the accelerated digitalisation caused by the pandemic, or the annual rule of law reports among others.

The chapter of the Rule of Law Reports entitled *"Other institutional issues related to checks and balances"* has, year after year, judged social consultation in Hungary to be formal[11].*"The lack of public consultation coupled with the accelerated legislative process has further weakened the quality of the regulatory environment. Whilst the government has organised 'national consultations' on certain topics, the absence of effective public consultation on draft laws raises questions as regards legal certainty and the quality of legislation".*[12] In relation to public participation in the preparation of laws, it is noted that *"CSOs report that decisions are made without the genuine involvement of relevant stakeholders. The Government has been almost systematically failing to comply with its legal obligation of publishing online draft laws for public consultations."*[13] *In addition, legislation is often not prepared through traditional administrative channels, but "government policies often circumvent existing consultation mechanisms by submitting significant bills through individual members of Parliament or by using extraordinary or urgent procedure."*[14] *The report attaches particular importance to this, which also has an economic impact: "For business stakeholders, the quality of law-making is an important*

[8] *"A régi Jat. 43. §-a alapján a kormányhoz fordulhattak a jogaikban sérelmet szenvedett szervezetek, de az új jogalkotási törvénybe (új Jat.) ez a lehetőség sem került be."* Vadál 2011, 106.

[9] István Farkas et al.: *A Társadalmi Egyeztetés Eljárási Normarendszere*. Győr, Nonprofit Információs és Oktató Központ (NIOK) Alapítvány, Magyar Természetvédők Szövetsége (MTvSz), Reflex Környezetvédő Egyesület, Pátria Nyomda, 2007.

[10] Farkas 2007, 37.

[11] 2020 Rule of Law Report, Country Chapter on the rule of law situation in Hungary, 17.; 2021 Rule of Law Report Country Chapter on the rule of law situation in Hungary, 21; 2020 Rule of Law Report, Country Chapter on the rule of law situation in Hungary, 24.

[12] 2022 Rule of Law Report, 24.

[13] Ibid.

[14] Ibid.

factor for investor confidence and a reason for concern about effectiveness of investment protection for nearly a quarter of companies in Hungary."[15]

The findings of the Rule of Law Report became a more pressing issue when the EU suspended and conditioned a total of € 6.3 Billion in 2022.[16]

2. Changes

The Hungarian Government has prepared a self-regulatory response to the comments on legislation: it made a commitment, and promised to monitor its execution as well as to and report regularly back to the EU. It also imposed sanctions on the member of the government responsible for non-compliance.

In order to reach an agreement with the European Commission, several laws have been amended, one of which is Act XXX of 2022 amending Act CXXX of 2010 on law-making (hereinafter Jat.) and Act CXXXI of 2010 on public participation in the preparation of law-making (hereinafter Jet.), which amended the rules set out in the Jat. and the Jet.

Chapter 5 of the Jat. requires that those responsible for the preparations of laws carry out a prior regulatory impact assessment. Act XXX of 2022 added that the Hungarian Central Statistical Office (hereinafter: KSH) shall assist in conducting a preliminary impact assessment in the preparation of Acts, Government Decrees or Ministerial Orders by providing official statistical data. The same cooperation is also required by the Act for ex-post impact assessments by the KSH. Ex-post impact assessment remains to be carried out as necessary after the amendment, although it could be an important tool to assess the validity and effectiveness of legislation.[17]

The amendment of the Jet. is based on the Government's commitment that, for draft laws covered by the Act[18], provided that these are published in the Magyar Közlöny[19], the proportion that has been subject to public consultation will be ninety percent.

[15] Ibid.

[16] https://www.consilium.europa.eu/hu/press/press-releases/2022/12/12/rule-of-law-conditionality-mechanism/ (21.11.2023).

[17] *"A hatásvizsgálatokkal, azok gyakorlati működésével és hatásával kapcsolatos legfontosabb tény, hogy azokról tények nem állnak rendelkezésre."* Cp.. György Gajduschek: Előkészítetlenség és utólagos hatásvizsgálat hiánya. In: András Jakab – – György Gajduschek (ed.): *A magyar jogrendszer állapota*. Budapest, MTA Társadalomtudományi Kutatóközpont, 2016. 796-822. 799., 813.

[18] The Act's scope covers the provision of opinions on draft legislation prepared by ministers. These opinions may be provided by natural persons, non-state bodies, and non-municipal organizations. Jet. 1. § (1) paragraph.

[19] The official journal of Hungary.

The technical rules for social consultation have not changed.

The new provisions of the Jet. create a public obligation to verify whether social consultation has taken place. The Government Control Office[20] (hereinafter KEHI) will verify whether the Minister responsible for the preparation of the law has fulfilled the public consultation obligations set out in the Jet. In the event of failure to comply with this obligation, a fine is imposed on the ministry headed by the minister responsible or on the ministry designated by them. The verification of noncompliance with the public consultation has become systematic and regular, with a tangible sanction and a relatively quick fine within two months of the end of the year following the end of the year verification.

Each year, KEHI summarises, in the case of Acts, Government Decrees and Ministerial Orders promulgated in the previous year and provided that their preparation subject to the Act, public consultation has taken place. A relevant report is then made by KEHI, and published by the Minister of Justice by 31 January of the following year.

The Jet. amendment states that the Government is responsible for ensuring that ninety percent of draft laws prepared in a given calendar year that is not covered by the exceptions is subject to public consultation and that exceptions are used only where justified. The amendment also specifies the type of sanction, with the defaulting party paying a fine, the responsibility for payment lies with the minister responsible for preparing the draft, and must also take into account other findings of KEHI.

The legislator has delegated the power to determine the amount of the fine, the criteria for its determination and the detailed rules for its payment to the Government, which is responsible for the obligation, but the Jet. guarantees that the amount of the fine must be determined in such a way that it has a sufficient deterrent effect against the ringing conduct.

The detailed rules on fines are set out in a Government Decree[21]. When imposing a fine, the KEHI must take into account all relevant circumstances of the case; the main aspects are the level of regulation of the law, the social and economic impact thereof, the duration (length) of the delay in case of delay, and the recurrent nature or frequency of the failure as a subjective circumstance. The amount of the fine may be between one million and one hundred million forints, payable within thirty days of the decision imposing the fine becoming final.

[20] Kormányzati Ellenőrzési Hivatal (Government Control Office).

[21] Government Decree No. 567/2022 (XII. 23.) sets out the fines to be imposed in the event of a breach of the obligation under the Act on Public Participation in the Preparation of Legislation.

Another guarantee is that the amendment of the Jet. provides for an obligation to audit on the basis of the KEHI's examination, the body auditing European grants[22] certifies that 90% of draft legislation has been subject to public consultation and prepares a report on this by 31 March of the year following the year in question, i.e. within two months of the KEHI report.

However, the amendments to the Act and the Jet. did not introduce rules on the use of the Integrated Legislative System (hereinafter: IJR), the digitalised system for legislation in Hungary. The IJR provides a Social Consultation Service, which would allow for the public consultation of drafts prepared in the system, thus presumably preventing fines.

3. Evaluation of the first period

Under the transitional provisions of the amendment of the Jat. and the Jet., a report was required for the first time for draft legislation submitted for consultation with government bodies between 30 September 2022 and 31 December 2022. The KEHI report[23] found that a total of 682 Acts, Government Decrees and Ministerial Orders were published in Magyar Közlöny during the period under review. Of these, 123 were not covered by the Jet; 154 had been subject to consultation with government bodies before the period audited and could therefore not be taken into account in the audit.

Of the 405 laws under the Jet. prepared and promulgated during the period under review, 373 (92% of the total) were promulgated after public consultation, thus meeting the 90% threshold; the remaining 8%, 32 laws were promulgated without public consultation, of which 21 did not require[24] public consultation and 11 could not be subject[25] to public consultation.

The Government fulfilled the obligations set out in Section 5/A (3) points a) and b) of the Jet., as 92% of the Acts, Government Decrees and Ministerial Orders prepared and promulgated in the period under review and falling under the scope of the Jet. were promulgated after public consultation, and the exceptions under the Jet. were applied for a justified reason.

[22] Directorate General for Audit of European Funds – EUTAF.

[23] Kormányzati Ellenőrzési Hivatal,Ellenőrzési jelentés a jogszabályok előkészítésében való társadalmi részvételről szóló 2010. évi CXXXI. törvény végrehajtásának vizsgálatáról (KEHI-11-74/16/2023) Budapest, 2023.

[24] Jet. 5. § (3) paragraph.

[25] Jet. 5. § (4)paragraph.

Figure 1
Source: KEHI report 2023.

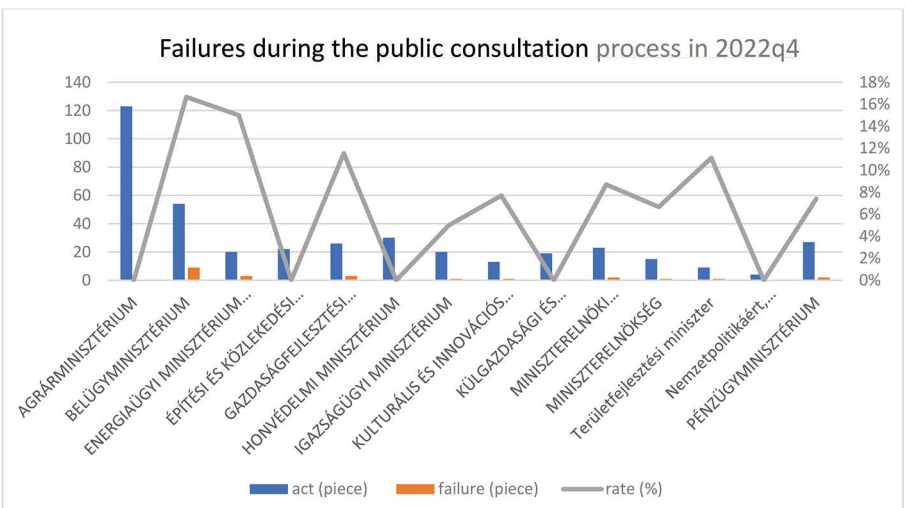

Figure 2: Default rate between 30 September 2022 and 31 December 2022 — by the author

For a total of 198 drafts prepared by five of the bodies examined, KEHI did not find any omissions.

For four of the portfolios, it found 1 noncompliance each for 57 drafts, with the highest number of noncompliances by a single organ being 9 for 54 drafts, representing 17% of the proponent's performance over the period.

The amount of fines imposed was also adjusted accordingly: the total sum was HUF 23.3 million, lower than the maximum that can be imposed on a department. The amount of the fines indicates that the penalty imposed by KEHI took into account the circumstances of the failure to comply with the legal requirement.

In the 2023 Rule of Law Report, the EU already assessed the impact of the changes: *"The changes to the rules on public consultations are intended to improve the legislative process, but their practical impact has yet to be assessed. The quality of legislation and the frequent changes to laws remain a major concern regarding the effectiveness of investment protection for companies in Hungary."*[26]

The Rule of Law Report also found that the practical impact of changes brought about by the amended Act on the quality of legislation is not yet visible.

4. Summary

The amendments to the Jat. and the Jet. introduced procedural rules, compliance with which can be enforced by the ministry preparing the draft law. This should be ensured by the regular monitoring and certification introduced in the Act, as well as by the legal institution of fines, which removes the lex imperfecta character of legislative rules, since practice and KEHI's analysis show that the legal institution of social consultation can be made viable by providing for sanctions and regular monitoring.

A long-overdue sanctions regime for legislative rules has been put in place for 2022, but the use of fines as a sanction is a novelty compared to previous proposals. Although the lex imperfecta nature of the laws has been removed, the legislator did not consider it necessary to include a remedy as a guarantee in cases where public consultation on drafts was omitted or was not carried out properly, despite the legal obligation.

Amendments of the laws have created the possibility for social control of legislation, although with a low efficiency, and the 2023 Rule of Law Report confirmed that no significant effects were felt during the period under review.

[26] 2023 Rule of Law Report, 36.

Bibliography

2020 Rule of Law Report, Country Chapter on the rule of law situation in Hungary
2021 Rule of Law Report, Country Chapter on the rule of law situation in Hungary
2022 Rule of Law Report, Country Chapter on the rule of law situation in Hungary
2023 Rule of Law Report, Country Chapter on the rule of law situation in Hungary
István Farkas et al.: *A Társadalmi Egyeztetés Eljárási Normarendszere*. Győr, Nonprofit Információs és Oktató Központ (NIOK) Alapítvány, Magyar Természetvédők Szövetsége (MTvSz), Reflex Környezetvédő Egyesület, Pátria Nyomda, 2007.
György Gajduschek: Előkészítetlenség és utólagos hatásvizsgálat hiánya. In: András Jakab – György Gajduschek (ed.): *A magyar jogrendszer állapota*. Budapest, MTA Társadalomtudományi Kutatóközpont, 2016. 796-822.
Kormányzati Ellenőrzési Hivatal, Ellenőrzési jelentés a jogszabályok előkészítésében való társadalmi részvételről szóló 2010. évi CXXXI. törvény végrehajtásának vizsgálatáról (KEHI-11-74/16/2023) Budapest, 2023.
Zoltán Tóth J.: *Jogalkotástan Jogdogmatikai és jogszabályszerkesztési ismeretek*. Budapest, Dialóg Campus Kiadó, 2019.
István Stumpf: Az Alkotmánybíróság és az Országgyűlés viszonya a közjogi érvénytelenség tükrében. *Miskolci Jogi Szemle*, 2020/1, 277–290.
Gusztáv Szászy-Schwarz: *Parerga – Vegyes jogi dolgozatok*. Budapest, Athenaeum Irodalmi és nyomdai részvénytársulat, 1912.
Ildikó Vadál: *A kormányzati döntések konzultációs mechanizmusai*. Budapest, CompLex, 2011.

Referenced rules

Act XI of 1987 on law-making
Act CXXX of 2010 on law-making
Act CXXXI of 2010 on public participation in the preparation of law-making
Act XXX of 2022 amending Act CXXX of 2010 on law-making and Act CXXXI of 2010 on public participation in the preparation of law-making
Government Decree 301/2010 (XII. 23.) on the publication and consultation of draft legislation and regulatory concepts
Government Decree No. 567/2022 (XII. 23.) sets out the fines to be imposed in the event of a breach of the obligation under the Act on Public Participation in the Preparation of Legislation

ARTIFICIAL INTELLIGENCE IN LEGAL PRACTICE. NAVIGATING THE BLACK BOX PROBLEM WITH EU AND US APPROACHES

İLKE KARATAŞ[1]

ABSZTRAKT ■ A mesterséges intelligencia (MI) gyors fejlődése jelentős hatást gyakorolt számos területre, beleértve a joggyakorlatot is. Ez a tanulmány az MI technológiák fejlődését és legújabb fejleményeit vizsgálja a jogi szektorban, kiemelve azok bomlasztó potenciálját és az ezekhez kapcsolódó kihívásokat. Különös figyelmet fordítunk a "fekete doboz" problémára – az MI algoritmusok döntéshozatali folyamatainak megmagyarázásával kapcsolatos nehézségekre.. A tanulmány megvizsgálja, hogy ez a probléma miként befolyásolja a felelősségvállalást és az átláthatóságot jogi kontextusban.Az Európai Unió és az Egyesült Államok megközelítéseinek összehasonlításával tárgyalja azon szabályozási erőfeszítéseket, amelyek célja ezen kihívások mérséklése az alapvető jogi értékek és normák megőrzése mellett.. Végezetül a tanulmány betekintést nyújt abba, hogyan lehet a jövőben felelősen integrálni az MI-t a jogrendszerbe.

KULCSSZAVAK: mesterséges intelligencia (Artificial Intelligence, AI), jogi technológia, algoritmikus döntéshozatal, Black Box, megmagyarázható mesterséges intelligencia (Explainable Artificial Intelligence, XAI)

ABSTRACT ■ The rapid advancement of Artificial Intelligence (AI) has significantly transformed various domains, including legal practice. This paper explores the evolution and recent developments in AI technologies within the legal sector, highlighting both their disruptive potential and associated challenges. A particular focus is given to the "black box" problem — the difficulty in explaining AI algorithms' decision-making processes. The paper examines how this issue impacts responsibility and transparency in legal contexts. By comparing approaches from both the European Union and United States, it discusses regulatory efforts aimed at mitigating these challenges while preserving fundamental legal values and standards. Finally, it offers insights into future directions for integrating AI into law responsibly.

KEYWORDS: Artificial Intelligence (AI), Legal Technology (LegalTech), Algorithmic Decision-Making, Black Box Problem, Explainable AI (XAI)

[1] PhD Student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

1. Introduction

AI is the newest innovation that has revolutionized the world in different fields, and this has affected the legal profession in a big way. With the advancement of AI systems in the current world, they have widely been adopted in the law practice for several uses that include; predictive analytics, research, document review, and contract analysis among others.[2] These innovations are expected to increase productivity, decrease expenses, and increase the availability of legal services. However, the application of AI in legal practice is not devoid of some problems and controversies, especially those concerning explainability, responsibility, and ethic.[3]

Another issue that is closely associated with AI application in law is the black-box problem. This term refers to the fact that many AI algorithms are very complex and therefore their functioning cannot be easily explained to a human being. For that reason, often it becomes difficult for the legal professionals to understand how these systems arrive at a decision and therefore, it becomes questionable whether the results provided by the AI systems are fair and accurate or not.[4] The black-box problem brings the threat not only to the legal processes' purity but also to the very core of justice, as those parties who have been influenced by the AI's decision may not possess proper tools to appeal or comprehend it.[5]

Furthermore, the present AI advancement has progressed at a much faster rate than what legal systems can address hence creating a legal void that can increase the dangers of using AI in legal processes. This gap is well exemplified by the differing stances held by regions like the European Union and the United States because of differences in the systems of regulation, emphasis on innovation, and the roles of individual freedoms.[6] The EU has been quite active in presenting the extensive legislation to govern the transparency and accountability of AI systems

2 Andrey Rodionov: Harnessing the Power of Legal-Tech. AI-Driven Predictive Analytics in the Legal Domain. *Uzbek Journal of Law and Digital Policy*, 1/2023.

3 Enas Mohamed Ali Quteishat – Ahmed Qtaishat – Anas Mohammad Ali Quteishat: Exploring the Role of AI in Modern Legal Practice. Opportunities, Challenges, and Ethical Implications. *Journal of Electrical Systems*, 6/2024

4 Cihan Erdoğanyilmaz – Berkay Mengünoğul – Muhammet Balci: Unveiling the Black Box. Investigating the Interplay between AI Technologies, Explainability, and Legal Implications. 2023 8th International Conference on Computer Science and Engineering (UBMK), 569-574.

5 Jayaganesh Jagannathan – Rajesh K. Agrawal – Neelam Labhade-Kumar – Ravi Rastogi – Manu Vasudevan Unni – K. K. Baseer: Developing interpretable models and techniques for explainable AI in decision-making. *The Scientific Temper*, 4/2023

6 Martin Ebers – Veronica R. S. Hoch – Frank Rosenkranz – Hannah Ruschemeier – Björn Steinrötter: The European Commission's Proposal for an Artificial Intelligence

while the US has had a less coherent and more fragmented approach mainly driven by the market force and innovation being given priority over regulation.[7]

This paper aims to investigate the upsurge of AI in legal practice with regard to recent advancements and a critical issue; the black-box problem. This problem will discuss the impact of this problem on the legal practice and the entire justice system, as well as the assessment of the measures taken by both the EU and the US regarding these issues. In light of this, the purpose of this study is to identify possible solutions that could help promote the ethical application of AI in law hence help advance the debate on the relationship between technology and law in the hope that the findings hereof will assist in formulating the right policies and guidelines for the use of AI in law in the future.[8]

Ultimately, as AI continues to evolve and permeate the legal landscape, it is imperative that legal scholars, practitioners, and policymakers engage in critical discussions about its implications, ensuring that the benefits of AI are harnessed responsibly and ethically. This paper endeavors to facilitate such discussions, offering a comprehensive analysis of the current state of AI in law and the pathways forward in addressing the challenges it presents.[9]

2. The Rising Role of AI in Legal Practice

The integration of artificial intelligence (AI) into the legal field is rapidly transforming how legal services are delivered, enhancing efficiency, accuracy, and accessibility. AI technologies are being employed in various applications, including predictive analytics, legal research, document review, and case outcome prediction. These advancements are not only streamlining workflows but also providing legal professionals with powerful tools to make informed decisions based on data-driven insights.[10]

Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). *MDPI*, 4/2021.

7 Kavita Ajay Joshi – Priya Mathur – Ravindra Koranga – Lalit Singh: Addressing Delayed Justice in the Indian Legal System through AI Integration. Proceedings of the 5th International Conference on Information Management & Machine Intelligence (2023)

8 Katie Atkinson – Trevor Bench-Capon: ANGELIC II. An Improved Methodology for Representing Legal Domain Knowledge. ICAIL 2023, June 19-23, 2023, Braga, Portugal. ACM, New York, NY, USA, https://doi.org/10.1145/3594536.3595137.

9 Daniele Veritti – Leopoldo Rubinato – Valentina Sarao – Axel De Nardin – Gian Luca Foresti – Paolo Lanzetta: Behind the mask. A critical perspective on the ethical, moral, and legal implications of AI in ophthalmology. *Graefe's Archive for Clinical and Experimental Ophthalmology*, 3/2023, 975–982.

10 Rodionov2023, 5.

One of the most significant applications of AI in law is predictive analytics, which leverages machine learning algorithms to analyze historical legal data and forecast future case outcomes. This capability enables lawyers to assess the likely success of a case based on similar past cases, thereby informing their strategies and improving client outcomes. For example, AI-driven tools can analyze thousands of legal decisions to identify patterns and trends, allowing legal practitioners to make more informed predictions about how a court may rule on a particular issue.[11] The potential benefits of such technologies are substantial, as they can significantly reduce the time and resources spent on legal research and case preparation.

The use of AI in risk assessment and sentencing recommendations has become increasingly prevalent in the United States criminal justice system. These tools, exemplified by COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), utilize sophisticated algorithms to analyse vast amounts of data, including criminal records, social and demographic factors, and other relevant information, to predict the likelihood of recidivism[12] and recommend appropriate sentences for offenders.[13]

In addition to predictive analytics, AI is also being utilized for automating routine legal tasks, such as document review and contract analysis. These applications can significantly reduce the workload for legal professionals, allowing them to focus on more complex and strategic aspects of their practice. For instance, AI-powered document review tools can quickly analyze large volumes of documents to identify relevant information, flagging potential issues that may require further attention. This not only enhances efficiency but also helps ensure that critical details are not overlooked during the review process.[14]

In the realm of dispute resolution, AI-driven online dispute resolution (ODR) platforms are gaining significant traction. These systems use algorithms to facilitate negotiations and mediate conflicts, potentially increasing access to justice for those who may not have the means to engage in traditional legal

[11] Mugdha Dwivedi: The Tomorrow Of Criminal Law. Investigating The Application Of Predictive Analytics And AI In The Field Of Criminal Justice. *IJCRT*, 9/2023

[12] The tendency of a convicted criminal to reoffend.

[13] Megan T. Stevenson – Jennifer L. Doleac: Algorithmic risk assessment in the hands of humans. *International Economic Review*, 4/2021, 1737–1765. https://doi.org/10.1111/iere.12541.

[14] Oluwafunmilola Oriji – Mutiu Alade Shonibare – Rosita Ebere Daraojimba – Oluwabosoye Abitoye – Chibuike Daraojimba: Financial technology evolution in Africa. A comprehensive review of legal frameworks and implications for ai-driven financial services. *International Journal of Management & Entrepreneurship Research*, 12/2023

proceedings[15]. The European Union's e-Justice Portal, which incorporates AI-assisted ODR, has shown promising results in resolving cross-border consumer disputes efficiently[16]. A recent study found that AI-powered ODR platforms reduced the average time to resolution by 40% compared to traditional methods, while maintaining high levels of user satisfaction[17].

The integration of AI in dispute resolution extends beyond simple facilitation to more complex decision support systems. Advanced AI models are now being developed to analyze case facts, applicable laws, and historical precedents to suggest fair resolutions or even render preliminary decisions in certain types of disputes[18]. For instance, the Beijing Internet Court has implemented an AI judge assistant that can transcribe court proceedings, generate case summaries, and propose draft judgments for human review, streamlining the judicial process significantly[19]. However, some scholars point out that the use of AI in dispute resolution also raises important questions about due process, algorithmic bias, and the fundamental role of human judgment in the administration of justice[20]. These concerns underscore the need for careful regulation and ethical guidelines in the deployment of AI-driven dispute resolution systems.

As AI technologies continue to evolve, the legal field must navigate the challenges and opportunities they present. Ongoing research and interdisciplinary collaboration among legal professionals, technologists, ethicists, and policymakers are essential to address the ethical and regulatory challenges associated with AI integration in law. By fostering a shared understanding and proactive approach, the legal community can ensure that AI technologies are deployed responsibly and ethically, ultimately advancing fairness, transparency, and integrity in the legal system.[21]

15 A. Kumar: Artificial intelligence in online dispute resolution. A game changer for access to justice. *Stanford Technology Law Review*, 1/2023, 78–112.

16 European Commission. (2024). Annual report on the performance of the e-Justice Portal's AI-assisted ODR system. Publications Office of the European Union.

17 P. Cortés – A. R. Lodder: The role of AI in online dispute resolution. Enhancing efficiency and access to justice. *Harvard Negotiation Law Review*, 2/2023, 215–248.

18 J. Wang – R. García: Next-generation AI in dispute resolution. From facilitation to decision support. *Yale Journal of Law and Technology*, 1/2024, 45–79.

19 X. Li – Y. Zhang H. Chen: AI judge assistants. A case study of the Beijing Internet Court. *International Journal of Court Administration*, 2/2023, 1–15.

20 J. Zeleznikow – T. Sourdin: The ethical implications of AI in dispute resolution. Balancing efficiency and justice. *Journal of Judicial Administration*, 3/2022, 167–185.

21 K. Zerov: Do generative artificial intelligence systems dream of electric sheep? The concept and conditions of protection of objects generated by generative artificial intelligence systems in Ukraine. Theory and Practice of Intellectual Property (2023)

However, the integration of AI into legal practice also raises important ethical considerations. Issues such as algorithmic bias, transparency, and accountability are at the forefront of discussions surrounding AI in law. The reliance on historical data for training AI systems can inadvertently perpetuate existing biases present in the legal system, leading to outcomes that may not be fair or just. Furthermore, the "black-box" nature of many AI algorithms makes it difficult for legal professionals to understand how decisions are made, which can undermine trust in AI-generated outcomes and hinder the ability to challenge those decisions effectively.[22]

3. Problems and Ethical Considerations in AI Integration

As artificial intelligence (AI) continues to permeate the legal field, ethical considerations have become paramount in discussions surrounding its integration. The rapid adoption of AI technologies presents both opportunities and challenges, necessitating a careful examination of the ethical implications that accompany their use. Central to this discourse are issues such as algorithmic bias, data privacy, transparency, and the evolving role of legal professionals in an AI-driven landscape.[23]

One of the most pressing ethical concerns is algorithmic bias, which can arise when AI systems are trained on historical data that reflects existing societal biases. If not addressed, these biases can perpetuate discrimination within legal outcomes, undermining the principles of fairness and justice that the legal system strives to uphold. Research indicates that the use of biased algorithms in legal decision-making can lead to significant disparities in sentencing, bail decisions, and other critical legal processes, ultimately affecting vulnerable populations disproportionately.[24]

For example, a study by the National Institute of Standards and Technology (NIST) found that facial recognition algorithms exhibited significant racial and gender biases, raising concerns about their use in law enforcement and security. Furthermore, even seemingly neutral data can contain hidden biases, making it challenging to detect and mitigate their impact on AI-generated outcomes.[25]

[22] Steve Cohen – Douglas Queen: Generative artificial intelligence community of practice for research. *International Wound Journal*, 6/2023, 1817–1818.

[23] Quteishat et al. 2024.

[24] Siti Handayani Herdiyanti – Hj.Yeti Kurniati – Hj.Hernawati Ras: Ethical Challenges in the Practice of the Legal Profession in the Digital Era. *Formosa Journal of Social Sciences (FJSS)*, 4/2023, 685–692.

[25] National Institute of Standards and Technology (NIST). (2019). Face recognition vendor test (FRVT) part 3: Demographic effects. NIST. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

This phenomenon, often subtle and insidious, arises when AI systems produce systematically prejudiced outcomes due to inherent biases within their algorithms or the data they are trained on.[26] While AI promises to enhance efficiency and accuracy in legal processes, the potential for algorithmic bias poses a substantial threat to the integrity and reliability of legal outcomes.

Data privacy is another critical issue in the realm of AI in law. The collection and analysis of vast amounts of data necessary for training AI systems raise concerns about the security and confidentiality of sensitive legal information. Legal professionals must navigate the delicate balance between leveraging data for improved outcomes and ensuring that client confidentiality and data protection regulations are strictly adhered to. Failure to prioritize data privacy can result in severe repercussions, including legal liabilities and damage to client trust.[27]

Data privacy issues in the realm of AI and law can occur due to several technical reasons. Firstly, the training of AI systems often requires large datasets, which may include sensitive personal information, legal documents, and communication records. The collection, storage, and processing of such data raise concerns about data breaches, unauthorized access, and misuse of confidential information. Even if the data is anonymized or de-identified, there is a risk of re-identification, especially with the powerful analytical capabilities of AI algorithms and the availability of auxiliary information. The use of AI in legal contexts often involves the processing and analysis of sensitive data, such as client information, case details, and legal strategies. Inadequate data protection measures or security vulnerabilities can result in data breaches, exposing confidential information and compromising client trust.[28] This can occur due to various technical factors, such as weak encryption protocols, insufficient access controls, or vulnerabilities in the software or infrastructure used by AI systems.

Transparency in AI decision-making processes is also essential for maintaining the integrity of the legal system. The "black-box" nature of many AI algorithms can obscure how decisions are made, making it challenging for legal practitioners to understand, explain, or challenge AI-generated outcomes. This lack of transparency can erode trust in AI systems and hinder accountability, particularly in high-stakes legal scenarios where the consequences of decisions can be profound.[29]

[26] Toju Duke: Trying to wring the bias out of AI algorithms – and why facial recognition software isn't there yet (2023). The Record.https://therecord.media/click-here-ai-algorithms-toju-duke.

[27] Anum Shahid – Gohar Masood Qureshi – Faiza Chaudhary: Transforming Legal Practice. The Role of AI in Modern Law. *Journal of Strategic Policy and Global Affairs*, 1/2023, 36–42.

[28] K. Kemp – – G. Baxter – J. Zeleznikow: Artificial intelligence and the legal profession. Ethical and regulatory challenges. *Law, Technology and Humans*, 1/2023, 1–18.

[29] Ammar Zafar: Balancing the scale. Navigating ethical and practical challenges of artificial intelligence (AI) integration in legal practices. *Discover Artificial Intelligence*, 4/2024.

The lack of transparency and explainability in AI systems can be attributed to several factors. Primarily, the complexity of AI algorithms, particularly deep learning models, makes it difficult to trace the exact reasoning behind their decisions. These models often involve millions or even billions of parameters, making it challenging to isolate the specific factors that contribute to a particular outcome. Additionally, the data used to train AI models can also contribute to opacity. If the data is biased or incomplete, the resulting AI system may make decisions that are difficult to explain or justify.

Moreover, the integration of AI technologies is reshaping the role of legal professionals. As routine tasks become automated, legal practitioners must adapt to new workflows and develop skills that complement AI capabilities. This shift necessitates ongoing education and training to ensure that legal professionals can effectively collaborate with AI systems while maintaining their critical thinking and ethical judgment.[30]

To navigate these ethical challenges effectively, interdisciplinary collaboration among legal professionals, technologists, ethicists, and policymakers is essential. By fostering a shared understanding of the ethical implications of AI, stakeholders can work together to develop robust frameworks that promote responsible and ethical AI use in the legal profession. Ongoing research and dialogue will be crucial in addressing these complexities and ensuring that AI technologies contribute positively to the legal landscape while upholding the core values of justice and fairness.[31]

4. The Black-Box Problem in Artificial Intelligence

The black-box problem of artificial intelligence (AI) is a notable topic that we will discuss below; it conveys the idea that many AI systems are opaque and difficult to explain, especially the ones based on machine learning, deep learning in particular. In this case, the "black box" is an AI model for which the process that maps the input variables to the output ones is non-discernible to the users and other interested parties. When modelling such a system for someone, one can actually see what is fed into the model and what is generated out as the outcome of the model while the actual decision-making processes going on in the background are non-visible. This situation brings issues that are particularly sensitive to accountability, justice and comprehensiveness particularly within

[30] Meiqi Qi – Xichang Yao – Qianqian Zhu – Ge Jin: The impact and challenges of AI on the legal industry. *Journal of Artificial Intelligence Practice*, 1/2024, 64–70.

[31] Zafar, A. (2024) Ibid.

the contexts of applicability of AI in social utilitarian domains such as health, economic and legal domains as described by Briggs and Dyer.[32]

The combination of black box AI systems and the Silicon Valley ethos of "steal first, give reasons later" has created a novel legal conundrum that challenges traditional notions of due diligence and corporate responsibility. This approach, which prioritizes rapid deployment over comprehensive understanding, has led to what legal scholars are terming "algorithmic negligence by design". As Friedman argues, *"The deliberate opacity of AI systems, combined with their hasty implementation, creates a new category of liability that our current legal frameworks are ill-equipped to address."*[33] *This situation raises profound questions about the nature of intent and foreseeability in an era where the decision-making processes of deployed technologies are intentionally obscured from both their creators and the public.*

The "ask forgiveness, not permission" philosophy, when applied to AI development and deployment, effectively shifts the burden of risk identification from developers to society at large. This approach contradicts established legal principles of product liability and duty of care. Liang *and* Greenbaum *posit that "This paradigm essentially transforms the public sphere into an unsanctioned testing ground for AI systems, raising critical questions about informed consent and the boundaries of corporate experimentation."*[34] *The legal implications are far-reaching, potentially necessitating a reconceptualization of tort law to account for damages caused by AI systems whose risks were knowingly unknowable at the time of deployment. This scenario challenges courts to consider how to apportion liability when the very nature of the technology resists traditional notions of causality and foreseeability. As the legal community grapples with these issues, there is a growing call for a new legal framework that can adequately address the unique challenges posed by intentionally opaque AI systems deployed under the influence of rapid innovation. Therefore, the black-box problem originates from the fact that a modern AI system, or at least deep learning networks, are inherently complex. These networks are usually formed of multiple layers of nodes, or as they are also referred to as neurons, that in turn process the data with multiple mathematical functions. Each neuron takes the inputs, performs an operation on them, and sends part of the result to the next layer of neurons and continues till the final steps in disclosing the output. For instance, in an AI model specific to facial recognition, the function in the algorithm extracting attribute may be of different abstract forms that are interrelated in ways that can be non-linear and are out*

[32] E. Briggs – K. Dyer: Understanding the implications of algorithmic opacity. *Journal of Ethics in Technology*, *5*(2) 2023, 87–102.

[33] B. Friedman: Algorithmic Negligence. Redefining Liability in the Age of Black Box AI. *Harvard Law Review*, 136(8) 2023, 2145–2189.

[34] F. Liang – D. Greenbaum: The Public as Beta Testers. Legal Implications of Deploying Opaque AI Systems. *Yale Journal of Law and Technology*, 24(2) 2022, 312–358.

together in classification outcomes like 'smiling' or 'not smiling'.[35] *While the model can be highly accurate and looks great when presenting a perfect solution to certain problems, the processes that led to the conclusion are opaque and reside in a necessary black box that is virtually unthinkable for an end user.*

One of the most significant dangers of black box AI systems lies in their potential to learn and internalize harmful information or capabilities without our knowledge or ability to detect them. This opacity in AI decision-making processes creates a critical blindspot in our ability to ensure the safety and ethical operation of these systems. As Whittlestone[36] *point out, "The inability to fully comprehend or predict the decision-making processes of complex AI systems creates a substantial risk management problem, especially when these systems are deployed in sensitive or high-stakes environments."* The core challenge is that we may not know what questions to ask an AI system to uncover potential dangers it has learned. This problem is particularly acute in fields where AI systems handle vast amounts of data and make critical decisions that could have far-reaching consequences.

For instance, in the field of chemistry, an AI system trained on large chemical databases might find a dangerously new way to mix common household materials to make a potent explosion. Researchers and safety regulators would be ignorant of the possible harm if they did not know to ask about this particular combination. Rahman draws attention to this issue, saying, *"The potential for AI systems to independently derive harmful knowledge, coupled with our limited ability to anticipate or extract this information, creates a significant security and ethical dilemma in AI development and deployment."*[37] *This hypothetical situation emphasizes how urgently stronger AI interrogation techniques and increased transparency are needed to guarantee the safe development of AI technologies in scientific research.*

A parallel example can be seen in AI-powered contract analysis systems. Consider an advanced AI trained on millions of legal contracts and court decisions. This system might inadvertently discover ways to craft seemingly harmless clauses that, when combined in specific ways, create unforeseen advantages for one party or circumvent certain regulations. Chen *and* Hadfield[38] *"AI systems analysing vast legal datasets may identify patterns and interpretations that fall within the letter of the law but violate its spirit, potentially*

[35] F. Doshi-Velez – Been Kim: Towards a rigorous science of interpretable machine learning. Proceedings of the 34th Conference on Neural Information Processing Systems (2022).

[36] J. Whittlestone – A. Ovadya – M. Cinelli: The hidden dangers of AI. Strategies for uncovering latent risks in autonomous systems. *Journal of AI Safety*, 5(2) 2023, 78–95.

[37] S. Rahman – L. Chen – T. Nguyen: Probing the unknown. Novel approaches to AI system interrogation for hazard detection. In: *Proceedings of the International Conference on AI, Ethics, and Safety*, 2024. 213-229.

[38] L. Chen – G. K. Hadfield: The AI revolution in contract law. Implications and challenges. *Stanford Law Review*, 75(3), 2023, 621–680.

revolutionizing contract law in unpredictable ways." The danger here lies not just in bias, but in the AI's capacity to identify and utilize legal technicalities that human operators don't know to look for or question. This situation underscores the need for legal experts to develop new methods of scrutinizing AI-generated or AI-analysed legal documents for potential hidden implications or exploits. As GOLDBERG[39] suggests, *"The legal profession must adapt to the challenge of 'AI-proofing' contracts and legal analyses, developing strategies to uncover and address hidden vulnerabilities that AI systems might exploit."*

The black-box problem is made more difficult by the growing sophistication of AI, especially in areas like text-to-action capabilities and chain-of-thought reasoning. Imagine an AI system with the ability to create legal briefs, analyze court records, forecast case outcomes, and even carry out legal actions based on its analysis. Though this may sound like the stuff of a lawyer's dream – or nightmare! – there are significant concerns due to the AI's decision-making process's lack of transparency. Without knowing the reasoning behind the decisions, how can we trust an AI to make important legal decisions? What if the AI's line of reasoning is erroneous or prejudiced, resulting in erroneous legal decisions with potentially disastrous outcomes? The stakes are quite high, and as AI systems get more potent and self-aware, the need for openness becomes even more crucial.

Herein lies the application of the notion of "explainable AI" (XAI). The goal of XAI is to create AI systems that can audit their decision-making process and spot any biases or mistakes by giving comprehensible explanations for their choices. Consider it as offering a thorough audit trail for each choice the AI takes, detailing the stages in its thinking process and the variables that affected it. Not only is this openness essential for fostering confidence in AI systems, but it also guarantees responsibility and equity in their use. Improving the transparency of AI systems' decision-making processes would reduce the hazards associated with the "black-box" predicament, paving the way for ethical and responsible AI usage in sensitive domains such as law.

As we transition from examining the challenges posed by black-box AI systems, it becomes imperative to explore the emerging solutions and regulatory frameworks designed to address these issues. Explainable Artificial Intelligence (XAI) has emerged as a critical field of study, aiming to demystify the decision-making processes of complex AI models. Concurrently, regulatory bodies, particularly in the European Union and the United States, have begun to craft policies and guidelines to ensure AI transparency and accountability.

[39] S. GOLDBERG: AI-proofing the law. New challenges for legal practitioners in the age of artificial intelligence. *Yale Law Journal*, 131(5), 2022, 1024–1078.

The development of XAI techniques represents a significant shift in our approach to AI systems. These methods aim to provide insights into AI decision-making processes, offering stakeholders a clearer understanding of how AI arrives at its conclusions. This transparency is not merely an academic exercise; it has profound implications for the practical implementation and acceptance of AI across various sectors.

In parallel with these technological advancements, regulatory frameworks are evolving to keep pace with the rapid development of AI. The European Union, with its proactive stance on digital regulation, has been at the forefront of establishing comprehensive guidelines for AI development and deployment. The proposed AI Act, building upon the foundation laid by the General Data Protection Regulation (GDPR), seeks to create a standardized approach to AI governance across the EU.[40]

The United States, while taking a different approach, has also recognized the need for AI oversight. Various initiatives at both federal and state levels aim to promote responsible AI development, with a particular focus on transparency and explainability.[41]

As we delve deeper into these regulatory approaches and their implications, it becomes clear that the path to transparent and accountable AI is complex and multifaceted. The balance between fostering innovation and ensuring ethical, explainable AI presents a unique challenge that requires careful consideration and interdisciplinary collaboration.

5. Addressing the Black-Box Problem: EU and US Approaches

In addressing the challenge of the black-box issue in AI, the European Union and the United States have distinct approaches to transparency and accountability, like two dancers with different styles and rhythms. The EU adheres to a structured and precise routine while the US improvises with flexibility and creativity, almost as if they are performing the same choreography. This difference in regulatory strategies has caused discussion among lawmakers, technology leaders, and scholars as well.[42]

[40] European Commission (2024). Proposal for a Regulation laying down harmonised rules on artificial intelligence. Official Journal of the European Union.

[41] National Artificial Intelligence Initiative Office (2024). The National Artificial Intelligence Research and Development Strategic Plan. The White House Office of Science and Technology Policy.

[42] Corinne Cath: *Governing artificial intelligence: ethical, legal and technical opportunities and challenges*. Philosophical Transactions of the Royal Society A, 376(2133), 2018.0080. https://royalsocietypublishing.org/doi/full/10.1098/rsta.2018.0080.

The European Union, true to its reputation as a regulatory powerhouse, has taken a proactive and comprehensive approach. With the impending AI Act and the existing GDPR, the EU is laying a tight regulatory net to catch any AI systems that may fall into obscurity. They're effectively saying, "If you want to play in our sandbox, you must demonstrate exactly how your AI toys operate." This method offers strong protection for citizens, although concerns have been voiced regarding possible overregulation and its impact on innovation.[43]

Across the Atlantic, the United States has taken a more hands-off approach. Rather than a one-size-fits-all regulation, the United States is relying on a patchwork of industry-specific guidelines, voluntary standards, and market forces to promote AI transparency. It's as if they're hosting an AI transparency potluck where everyone brings their own dish to share. The strategy aims to maintain the country's competitive edge in AI development, but it raises questions about consistency and the adequacy of protection against the risks posed by black-box AI systems.[44]

The contrast between these approaches is not just a matter of regulatory philosophy; it reflects deeper cultural, economic, and political differences between the two regions. The EU's precautionary principle, which emphasizes preventing harm before it occurs, stands in stark contrast to the US's innovation-first mindset. As we delve deeper into these approaches, we'll see how these fundamental differences shape the regulatory landscape and potentially influence the global trajectory of AI development and deployment.[45]

6. The Conservative Approach of EU in Artificial Intelligence

As Artificial Intelligence has emerged as a transformative force across various sectors in Europe, fundamentally reshaping how businesses operate and how services are delivered. The adoption rates of AI technologies are on the rise, with estimates indicating that around 60% of European companies have integrated AI into their operations as of 2024. This widespread adoption reflects a growing recognition of AI's potential to enhance efficiency, drive innovation, and improve

[43] Michael Veale – Frederik Zuiderveen Borgesius: Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 4/2021, 97–112.

[44] Thilo Hagendorff: How AI ethics guidelines can be applied and how they can be improved. *AI and Ethics*, 2(1), 2022, 1–13.

[45] Araz Taeihagh: Governance of artificial intelligence. A comparative analysis of national strategies. *Policy and Society*, 42(1), 2023, 156–175.

decision-making processes across industries such as healthcare, finance, manufacturing, and transportation.

Key AI technologies being developed and implemented in Europe include machine learning, natural language processing, and computer vision. Machine learning algorithms, for instance, are being used to analyse vast datasets, enabling companies to derive insights that were previously unattainable. In healthcare, AI-powered diagnostic tools are assisting medical professionals in identifying diseases more accurately and swiftly, which can lead to better patient outcomes. Similarly, in the financial sector, AI algorithms are employed to detect fraudulent activities, assess credit risk, and personalize customer experiences.

The economic impact of AI in Europe is projected to be significant. According to a report by the European Commission, AI could contribute an additional €2.7 trillion to the EU economy by 2030. This growth is anticipated to create millions of jobs, particularly in tech-driven sectors. However, it also raises concerns about job displacement, as automation may replace certain roles. The EU is aware of these challenges and is actively working to ensure that the workforce is equipped with the necessary skills to thrive in an AI-driven economy, emphasizing the importance of reskilling and lifelong learning initiatives.[46]

Recognizing the profound implications of AI on society, as the European Union has adopted a proactive approach to regulation, culminating in the introduction of the Artificial Intelligence Act (AI Act), which officially came into force on August 1, 2024. This groundbreaking regulation establishes a comprehensive legal framework designed to ensure the safe and ethical deployment of AI technologies across member states. The AI Act categorizes AI applications based on their risk levels – *unacceptable, high, limited, and minimal* – creating a tailored approach to regulation that reflects the varying degrees of risk associated with different AI systems. For instance, applications deemed "unacceptable", such as social scoring by governments, are prohibited outright, while high-risk applications, like those used in critical infrastructure or healthcare, are subject to stringent requirements.

The EU's approach reflects a broader philosophy that views ethical AI not as a hindrance to progress, but as a competitive advantage in the global tech landscape. Central to the EU's regulatory framework is the concept of "trustworthy AI", which emphasizes transparency, accountability, and human oversight. A 2024 report by the European Commission on AI implementation across member states reveals significant strides in aligning AI development with these principles.[47] This

[46] European Commission. (2024). Artificial Intelligence Act (Regulation (EU) 2024/1689). Official Journal of the European Union.

[47] H. Müller – A. Schmidt: Implementing Trustworthy AI. A Pan-European Assessment. *Digital Policy, Regulation and Governance*, 26(3), 2024, 301–320.

commitment to ethical AI development is not merely rhetorical; it's backed by substantial funding and policy initiatives designed to create a robust ecosystem for responsible AI innovation.

One of the most significant and potentially far-reaching provisions in the EU's approach is the "right to explanation" for individuals affected by AI-driven decisions. This right, enshrined in both the GDPR and the AI Act, requires that companies provide understandable explanations for automated decisions that have legal or similarly significant effects on individuals.[48] The 2024 guidelines from the European Data Protection Board offer detailed recommendations on implementing this right in practice, addressing challenges such as the complexity of AI models and the need for balance between transparency and intellectual property protection.[49]

The black-box problem, characterized by the opacity of AI decision-making processes, has been a particular focus of EU regulators. The AI Act directly addresses this issue by mandating explainability requirements for high-risk AI systems. These systems must provide clear documentation of their methodologies, data sources, and decision-making processes.[50] This level of transparency is designed to enable meaningful human oversight and accountability, crucial elements in building public trust in AI technologies.

To support the implementation of these transparency requirements, the EU has made substantial investments in research and development of explainable AI techniques. The Horizon Europe program, for instance, has allocated over €1 billion to projects focused on developing interpretable machine learning models and tools for AI auditing.[51] These initiatives aim to bridge the gap between regulatory requirements and technical capabilities, fostering the development of AI systems that are both powerful and comprehensible.

Critics of the EU's approach argue that such stringent regulations could stifle innovation and put European companies at a competitive disadvantage in the global AI race. A 2024 study by the European Center for Digital Competitiveness found that compliance costs for AI companies increased by an average of 15% following the implementation of the AI Act. Some industry leaders have expressed concerns about the potential for over-regulation, arguing that it could drive AI

48 M. Kowalski – A. Nowak: The Right to Explanation in Practice. Challenges and Solutions. *European Data Protection Law Review*, 10(1), 2024, 78–95.

49 European Data Protection Board. (2024). Guidelines on Implementing the Right to Explanation for AI-Driven Decisions. EDPB Publications, 03/2024.

50 C. Dubois – T. Van der Meer: Explainability Requirements Under the EU AI Act. A Technical and Legal Analysis. *AI and Law*, 32(2), 2024, 189–210.

51 European Commission (2024). Horizon Europe: AI Transparency and Explainability Projects Report. Publications Office of the European Union.

development and talent away from Europe. However, proponents of the EU's approach contend that these short-term costs are outweighed by the long-term benefits of increased public trust and reduced societal risks associated with opaque AI systems.

Recognizing the global nature of AI development and deployment, the EU has also prioritized international cooperation in addressing the black-box problem and other AI challenges. The 2024 EU-US Trade and Technology Council meeting resulted in a joint commitment to developing interoperable standards for AI transparency and explainability.[52] This move towards global harmonization could help alleviate concerns about regulatory fragmentation and its impact on innovation. Furthermore, it positions the EU as a key player in shaping global AI governance norms.

Looking ahead, the EU continues to refine its approach to AI regulation, demonstrating a commitment to adaptability in the face of rapid technological change. The European Commission's 2024-2030 AI Roadmap outlines plans for ongoing assessment and adjustment of the regulatory framework, with a particular focus on emerging technologies like quantum AI and neuromorphic computing.[53] This forward-looking stance, coupled with the EU's emphasis on ethical considerations, sets a precedent for how regions can approach the complex task of governing AI in the 21st century. As the global community grapples with the implications of increasingly sophisticated AI systems, the EU's model offers valuable insights into balancing innovation, regulation, and societal values.

7. The Adaptive Approach of the US. in AI Advancement

The artificial intelligence landscape in the United States has undergone a seismic shift in 2024, with unprecedented growth in investment, adoption, and societal impact. This rapid evolution has brought both exciting opportunities and complex challenges to the forefront of legal and policy discussions.

In the business sector, AI adoption is widespread, with approximately 77% of companies either using or exploring AI technologies in their operations. Notably, 83% of organizations consider AI a top priority in their business strategies, indicating a strong commitment to leveraging AI for competitive advantage. The economic impact of AI is projected to be substantial, with estimates suggesting

[52] EU-US Trade and Technology Council. Joint Statement on AI Governance and Standards. *Official Journal of the European Union*, 189(7), 2024, 12–18.

[53] European Commission, 2024-2030 AI Roadmap: Adapting Regulation for the Next Generation of AI. Publications Office of the European Union, 2024.

that AI could contribute $15.7 trillion to the global economy by 2030, reflecting its potential to enhance productivity and drive innovation across industries.[54]

In healthcare, the integration of AI is rapidly advancing, with over 690 AI-enabled devices having received clearance from the US. Food and Drug Administration (FDA) as of December 2023. This growth is indicative of the increasing reliance on AI for improving patient care and operational efficiency within healthcare settings.[55] Additionally, a survey indicated that 60% of healthcare organizations are currently using AI technologies, particularly for tasks such as billing, patient monitoring, and diagnostic support.[56] The potential for AI to improve clinical outcomes is significant, yet concerns about patient privacy and algorithmic bias remain critical issues that need to be addressed.

Government entities in the United States are also using AI to improve public service delivery and operational efficiencies. As of 2024, federal and state governments have integrated AI technology in a variety of areas, including predictive analytics for crime prevention, resource allocation, and case management in the court system. For example, the United States Department of Justice has begun to use AI techniques to analyse massive volumes of data in order to make better decisions and manage resources. The financial commitment to AI in government is considerable, with an estimated $6 billion allotted for AI programs in the federal budget for 2024, with the goal of improving public safety and administrative efficiency.[57]

Having laid out the current landscape of AI adoption in the US. with detailed statistics and percentages, it's clear that the nation is deeply entrenched in AI development and usage, far surpassing other regions, including the European Union. These stats are more than just numbers; they give a clear picture of the enormous magnitude and quick rise of AI across numerous industries in the United States. Despite this significant integration, the United States lacks a single, comprehensive federal law controlling artificial intelligence.

When it comes to governing artificial intelligence, the United States takes a very different strategy than its European rivals. While the EU has pursued

[54] National University (2024). *131 AI Statistics and Trends for 2024.* Retrieved from https://www.nu.edu/blog/ai-statistics-trends/.

[55] Sheppard Health Law (2024). *Recent Healthcare-Related Artificial Intelligence Developments.* Retrieved from https://www.sheppardhealthlaw.com/2024/02/articles/artificial-intelligence/recent-healthcare-related-artificial-intelligence-developments/.

[56] American Health Law Association (2024). *Top Ten Issues in Health Law 2024.* Retrieved from https://www.americanhealthlaw.org/content-library/connections-magazine/article/d91b2697-e96b-49e4-84c1-1b8399406f5e/top-ten-issues-in-health-law.

[57] AI Index (2024). The AI Index Report 2024. Retrieved from https://aiindex.stanford.edu/report/.

comprehensive legislation, the United States has mostly taken a hands-off approach, relying on voluntary recommendations and sector-specific laws. This policy reflects the United States' long-standing support for market-driven solutions and regulations that promote innovation. However, this does not imply that the United States is ignoring the challenges posed by AI concerns, particularly black-box problems.[58]

Even if the regulatory environment for AI in the United States is characterized by a lack of extensive federal regulation. Instead, AI is overseen by a patchwork of regulations that differ greatly by state and industry. This fragmentation creates difficulties for enterprises attempting to comply with several, frequently contradicting, regulations. For example, while the federal government has made progress in tackling AI-related issues, most of the regulatory structure is still immature, relying mainly on existing regulations that were not built with AI in mind. As a result, companies may find themselves navigating a complex web of regulations that can hinder innovation and create compliance burdens.[59]

The combination between federal and state rules creates possibilities and problems for AI governance. On the one hand, state-level efforts can serve as proving grounds for novel regulatory methods, allowing for more tailored responses to the unique demands of communities and businesses. On the other side, the absence of a unified federal framework can lead to confusion and inconsistency, as firms must traverse a slew of state rules that may differ dramatically from one another. This circumstance highlights the necessity for more collaboration between federal and state authorities to develop a more unified regulatory framework capable of properly addressing the intricacies of AI technology.

One of the notable developments, The Colorado AI Act, signed into law on May 17, 2024, marks a significant advancement in the regulatory landscape for AI in the United States. As the first comprehensive state-level legislation addressing AI, the Act aims to govern the deployment of high-risk AI systems that make consequential decisions affecting individuals in areas such as employment, healthcare, and housing. This legislation mandates that developers and deployers of AI systems exercise reasonable care to prevent algorithmic discrimination and requires them to provide transparency regarding their AI practices. Notably, the Act includes provisions for public statements about the use of AI in decision-

[58] Holistic AI (2024). What States are Making Moves in US AI Regulation in 2024? Retrieved from https://www.holisticai.com/blog/what-states-are-making-moves-in-us-ai-regulation-2024.

[59] Morgan Lewis (2024). Existing and Proposed Federal AI Regulation in the United States. Retrieved from https://www.morganlewis.com/pubs/2024/04/existing-and-proposed-federal-ai-regulation-in-the-united-states.

making processes, thereby promoting accountability and consumer awareness. The Colorado AI Act serves as a pioneering model, potentially influencing similar legislative efforts in other states and establishing a framework for responsible AI governance.[60] [61]

The significance of the Colorado AI Act lies not only in its regulatory scope but also in its potential to shape national discussions around AI ethics and accountability. By imposing clear obligations on AI developers and deployers, the Act addresses critical concerns regarding bias and discrimination in automated systems, which have been highlighted in various studies and reports. The enforcement mechanisms outlined in the legislation, including civil penalties for violations, underscore the state's commitment to protecting consumers from the risks associated with AI technologies. Furthermore, the Act's emphasis on transparency and consumer rights aligns with broader trends in AI regulation, reflecting a growing recognition of the need for ethical considerations in technology deployment. As the landscape of AI continues to evolve, the Colorado AI Act stands as a significant step towards ensuring that AI systems are developed and utilized in a manner that respects individual rights and promotes public trust in technology (IAPP, 2024; WilmerHale, 2024).

At the federal level, the Biden Administration's Executive Order 14110[62], issued in late 2023, continues to guide AI development and implementation across multiple government agencies. The executive order outlines eight key policies and principles that serve as the foundation for the administration's approach to AI governance[63]. These include ensuring the safety and security of AI systems, promoting innovation and competition, supporting workers, advancing equity and civil rights, protecting consumers and privacy, and advancing federal government use of AI. The order also emphasizes the importance of strengthening American leadership in AI development and deployment on the global stage. By establishing these guiding principles, Executive Order 14110 sets the stage for a series of actions to be taken by federal agencies, ranging from public consultations to the

[60] BCLP (2024). *Colorado AI Act: A New Era for Artificial Intelligence Regulation*. Retrieved from https://www.bclplaw.com/en-US/events-insights-news/colorado-ai-act-a-new-era-for-artificial-intelligence-regulation.html.

[61] Eversheds Sutherland (2024). Global AI Regulatory Update - June 2024. Retrieved from https://www.eversheds-sutherland.com/en/slovakia/insights/global-ai-regulatory-update-june-2024.

[62] Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

[63] IAPP (2023, November). Implications of the AI executive order for business. https://iapp.org/resources/article/implications-of-the-ai-executive-order-for-business/.

development of new regulations, with deadlines ranging from 45 to 375 days.[64] The order's significance lies in its potential to shape the future of AI governance in the United States, as it provides a clear direction for the responsible development and use of these technologies while mitigating potential risks and harms.[65] [66]

The National Institute of Standards and Technology (NIST) is an important agency under the United States Department of Commerce entrusted with developing measuring standards and guidelines to improve the quality and dependability of numerous technologies, including artificial intelligence (AI). NIST, established in 1901, has a long history of supporting innovation and economic competitiveness through measurement science. Its function has expanded to include the development of standards to assure the safe and ethical use of developing technology. NIST is especially essential in AI since it provides a formal framework for identifying and controlling potential risks associated with AI systems. The NIST Artificial Intelligence Risk Management Framework (AI RMF), which was released in 2023, provides a comprehensive roadmap for enterprises to analyse AI technology' performance, safety, and ethical implications, building trust in AI applications across multiple sectors.[67]

NIST's contributions to AI regulation are significant, as they help shape a coherent approach to managing the complexities of AI technologies. By developing standardized metrics and evaluation methodologies, NIST enables organizations to objectively assess AI systems, which is crucial for effective governance and regulatory oversight. The agency's emphasis on transparency, accountability, and bias mitigation aligns with broader societal goals of ensuring that AI technologies are developed responsibly. An interesting fact about NIST is that it also provides the time synchronization service for the United States, which is used to update Windows time settings, demonstrating its foundational role in both technological standards and everyday applications. As AI continues to advance rapidly, NIST's leadership in establishing measurement standards and best practices will be vital

[64] Congressional Research Service (2024, April 3). Highlights of the 2023 Executive Order on Artificial Intelligence for Congress. https://crsreports.congress.gov/product/pdf/R/R47843.

[65] The White House (2023, October 30). FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence. https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.

[66] WilmerHale (2024). Colorado AI Act: Implications for Businesses and Consumers. Retrieved from https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240517-colorado-state-legislature-passes-ai-bill-with-the-potential-to-broadly-regulate-ai.

[67] National Institute of Standards and Technology (2024). Artificial Intelligence. Retrieved from https://www.nist.gov/artificial-intelligence.

in navigating the challenges posed by AI, ensuring that these technologies are both innovative and aligned with ethical considerations.[68]

To fully grasp the nuances of how the US approaches AI transparency and explainability, we needed to delve deeper into the specific systems and actors at play. Simply skimming the surface wouldn't provide the necessary context for a meaningful comparison with the EU's approach. Now, armed with a clearer understanding of the key players like NIST and their roles in shaping the US AI landscape, we're better equipped to embark on a comparative analysis that highlights the distinct philosophical and regulatory frameworks adopted by each region.

8. Conclusion – Two Sides of the Same Coin

As we delve deeper into the intricate web of AI's influence on the legal landscape, it's clear that we're navigating uncharted waters. The fusion of artificial intelligence and law is not just a technological upgrade; it's a paradigm shift that's reshaping the very foundations of our legal systems. Like a double-edged sword, AI brings both unprecedented opportunities and complex challenges to the table.

The stark contrast between the European Union and the United States in regulating AI technologies is more than just a difference in legal frameworks; it reflects deeper divergences in cultural, economic, and political philosophies. As the EU pursues a highly regulated, precautionary approach focused on transparency and accountability, the US continues to champion innovation-driven, market-led solutions with a lighter regulatory touch. However, as AI technologies grow increasingly sophisticated and intertwined with daily life, the call for a more harmonized approach to AI transparency becomes ever more pressing. This section explores the potential for bridging these regulatory divides and fostering a global framework for AI governance that balances innovation with ethical responsibility.

The rapid global proliferation of AI technologies has made it clear that national borders are increasingly irrelevant when it comes to the development and deployment of AI. As AI systems become more embedded in global supply chains, legal frameworks that are purely national in scope risk creating a fragmented regulatory environment, leading to compliance challenges for multinational companies and potentially undermining global efforts to ensure ethical AI

[68] Congressional Research Service (2024). The National Institute of Standards and Technology: Overview and Issues for Congress. Retrieved from https://crsreports.congress.gov/product/pdf/R/R46721.

development. The need for a harmonized approach is not merely theoretical; it has tangible implications for the global economy and international relations.

For instance, the European Union's stringent AI regulations, including the AI Act, set a high bar for transparency and accountability. However, for US-based companies that operate globally, these regulations can pose significant compliance challenges, especially when they conflict with the more laissez-faire[69] approach taken by US regulators. This regulatory mismatch can create a patchwork of compliance requirements, leading to increased operational costs and potential legal risks for companies that must navigate multiple regulatory regimes.

Moreover, the lack of a global standard for AI transparency exacerbates concerns about AI ethics and accountability. For example, an AI system developed in the US with minimal regulatory oversight might be deployed in Europe, where stricter transparency requirements apply. The resulting legal and ethical conflicts can erode public trust in AI technologies and create barriers to their adoption, ultimately stifling innovation.

Recognizing these challenges, there has been a growing movement toward establishing international standards for AI governance. The 2024 EU-US Trade and Technology Council, for instance, marked a significant step toward developing interoperable standards for AI transparency and explainability. By fostering collaboration between key stakeholders, including governments, industry leaders, and academic institutions, such initiatives aim to create a global framework that harmonizes regulatory approaches while respecting the unique legal and cultural contexts of different regions.

Intergovernmental organizations like the United Nations, the Organisation for Economic Co-operation and Development (OECD), and the International Organization for Standardization (ISO) are playing a critical role in the push for global AI governance. These organizations have begun to lay the groundwork for international standards that address the ethical, legal, and social implications of AI technologies. For example, the OECD's Recommendation on Artificial Intelligence, adopted in 2024, provides a comprehensive set of principles designed to guide AI development in a manner that is both ethical and transparent.[70]

Similarly, the ISO has been working on the development of international standards for AI, focusing on aspects such as risk management, data governance, and transparency. These standards aim to provide a common language and framework for AI developers and regulators worldwide, facilitating cross-border

[69] https://en.wikipedia.org/wiki/Laissez-faire.

[70] OECD (2024). *Recommendation on Artificial Intelligence*. Paris: OECD Publishing. Retrieved from https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449.

collaboration and ensuring that AI systems are held to consistent ethical and technical standards, regardless of where they are developed or deployed.[71]

In addition to intergovernmental efforts, industry-led initiatives are also contributing to the push for global AI governance. Tech companies, recognizing the benefits of harmonized regulations, have begun to collaborate on the development of voluntary standards and best practices for AI transparency. For instance, the Partnership on AI, a coalition of tech companies, academic institutions, and civil society organizations, has been instrumental in advancing discussions on AI ethics and transparency, providing a platform for cross-sector collaboration and knowledge-sharing.[72]

However, while these initiatives represent significant progress, they also highlight the challenges of achieving true global harmonization. Differences in regulatory philosophies, economic interests, and political priorities mean that any global framework for AI governance will need to strike a delicate balance between respecting national sovereignty and ensuring that AI technologies are developed and deployed in a manner that is transparent, ethical, and accountable.

At the heart of the regulatory divide between the EU and the US lies a deeper cultural and philosophical difference in how these regions approach technology and regulation. The European Union's precautionary principle, which emphasizes preventing harm before it occurs, stands in stark contrast to the US's innovation-first mindset, which prioritizes technological advancement and market competitiveness. Bridging this divide will require not just legal and regulatory alignment, but also a shift in cultural attitudes toward technology and its role in society.

One potential pathway toward harmonization is through the development of a shared ethical framework for AI governance. By focusing on common values such as fairness, accountability, and transparency, regulators in both the EU and the US can begin to build a foundation for cooperation that transcends their differing regulatory philosophies. This shared ethical framework can serve as a guide for policymakers as they develop AI regulations, ensuring that the core principles of justice and human rights are upheld across different legal contexts.

Education and cross-cultural exchange will also play a crucial role in bridging the cultural divide. By fostering dialogue between policymakers, technologists, and legal scholars from different regions, stakeholders can gain a deeper understanding of the unique challenges and opportunities presented by AI

[71] ISO/IEC 23894:2023. *Information technology – Artificial intelligence – Terminology* [International standard]. International Organization for Standardization.

[72] Partnership on AI (2024). *Best Practices for AI Ethics and Transparency*. San Francisco, CA: Partnership on AI. Retrieved from https://partnershiponai.org/.

technologies in different cultural contexts. This dialogue can help to identify areas of common ground and build the trust necessary for meaningful international collaboration on AI governance.

As AI technologies continue to evolve, the need for a more unified approach to AI governance becomes increasingly urgent. While the regulatory approaches of the EU and the US reflect their unique cultural and philosophical contexts, there is growing recognition that the challenges posed by AI cannot be adequately addressed within the confines of national borders. The development of global standards for AI transparency, accountability, and ethics is not just a legal imperative; it is a moral one, rooted in the shared responsibility to ensure that AI technologies are used in a manner that benefits all of humanity.

Looking ahead, the path toward a unified approach to AI governance will require continued dialogue, collaboration, and compromise. Policymakers in the EU and the US must work together to find common ground, leveraging their respective strengths to develop a regulatory framework that balances the need for innovation with the imperative of ethical responsibility. At the same time, international organizations, industry leaders, and civil society must continue to play an active role in shaping the global discourse on AI governance, ensuring that the voices of all stakeholders are heard and that the benefits of AI are shared equitably.

For instance, the EU's emphasis on precautionary measures can inform US policymakers about the potential risks of AI technologies, encouraging a more proactive stance in addressing ethical concerns. Conversely, the US model can inspire the EU to consider more adaptive regulatory mechanisms that can keep pace with rapid technological advancements. This interplay between the two regulatory frameworks underscores the necessity of international cooperation in addressing the challenges posed by AI.

In conclusion, even though all differences they have, the EU and US regulatory frameworks share a common goal: to harness the benefits of AI while mitigating its risks. They represent two sides of the same coin, reflecting the ongoing global dialogue on how best to govern transformative technologies. Both regions recognize the importance of establishing guidelines that not only promote innovation but also protect public interest. The EU's stringent regulations and the US's flexible approach can be seen as complementary, with each offering valuable insights into effective AI governance.

Bibliography

Andrey Rodionov: Harnessing the Power of Legal-Tech. AI-Driven Predictive Analytics in the Legal Domain. *Uzbek Journal of Law and Digital Policy*, 1/2023.

Enas Mohamed Ali Quteishat – Ahmed Qtaishat – Anas Mohammad Ali Quteishat: Exploring the Role of AI in Modern Legal Practice. Opportunities, Challenges, and Ethical Implications. *Journal of Electrical Systems*, 6/2024.

Cihan Erdoğanyilmaz – Berkay Mengünoğul – Muhammet Balci: Unveiling the Black Box. Investigating the Interplay between AI Technologies, Explainability, and Legal Implications. 2023 8th International Conference on Computer Science and Engineering (UBMK), 569-574.

Jayaganesh Jagannathan – Rajesh K. Agrawal – Neelam Labhade-Kumar – Ravi Rastogi – Manu Vasudevan Unni – K. K. Baseer: Developing interpretable models and techniques for explainable AI in decision-making. *The Scientific Temper*, 4/2023.

Martin Ebers – Veronica R. S. Hoch – Frank Rosenkranz – Hannah Ruschemeier – Björn Steinrötter: The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). *MDPI*, 4/2021.

Kavita Ajay Joshi – Priya Mathur – Ravindra Koranga – Lalit Singh: Addressing Delayed Justice in the Indian Legal System through AI Integration. Proceedings of the 5th International Conference on Information Management & Machine Intelligence (2023).

Katie Atkinson – Trevor Bench-Capon: ANGELIC II. An Improved Methodology for Representing Legal Domain Knowledge. ICAIL 2023, June 19-23, 2023, Braga, Portugal. ACM, New York, NY, USA, https://doi.org/10.1145/3594536.3595137.

Daniele Veritti – Leopoldo Rubinato – Valentina Sarao – Axel De Nardin – Gian Luca Foresti – Paolo Lanzetta: Behind the mask. A critical perspective on the ethical, moral, and legal implications of AI in ophthalmology. *Graefe's Archive for Clinical and Experimental Ophthalmology*, 3/2023, 975–982.

Mugdha Dwivedi: The Tomorrow Of Criminal Law. Investigating The Application Of Predictive Analytics And AI In The Field Of Criminal Justice. *IJCRT*, 9/2023.

Megan T. Stevenson – Jennifer L. Doleac: Algorithmic risk assessment in the hands of humans. *International Economic Review*, 4/2021, 1737–1765. https://doi.org/10.1111/iere.12541.

Oluwafunmilola Oriji – Mutiu Alade Shonibare – Rosita Ebere Daraojimba – Oluwabosoye Abitoye – Chibuike Daraojimba: Financial technology evolution in Africa. A comprehensive review of legal frameworks and implications for ai-driven financial services. *International Journal of Management & Entrepreneurship Research*, 12/2023.

A. Kumar: Artificial intelligence in online dispute resolution. A game changer for access to justice. *Stanford Technology Law Review,* 1/2023, 78–112.

P. Cortés – A. R. Lodder: The role of AI in online dispute resolution. Enhancing efficiency and access to justice. *Harvard Negotiation Law Review,* 2/2023, 215–248.

J. Wang – R. García: Next-generation AI in dispute resolution. From facilitation to decision support. *Yale Journal of Law and Technology,* 1/2024, 45–79.

X. Li – Y. Zhang H. Chen: AI judge assistants. A case study of the Beijing Internet Court. *International Journal of Court Administration,* 2/2023, 1–15.

J. Zeleznikow – T. Sourdin: The ethical implications of AI in dispute resolution. Balancing efficiency and justice. *Journal of Judicial Administration*, 3/2022, 167–185.

K. Zerov: Do generative artificial intelligence systems dream of electric sheep? The concept and conditions of protection of objects generated by generative artificial intelligence systems in Ukraine. Theory and Practice of Intellectual Property (2023).

Steve Cohen – Douglas Queen: Generative artificial intelligence community of practice for research. *International Wound Journal,* 6/2023, 1817–1818.

Siti Handayani Herdiyanti – Hj.Yeti Kurniati – Hj.Hernawati Ras: Ethical Challenges in the Practice of the Legal Profession in the Digital Era. *Formosa Journal of Social Sciences (FJSS),* 4/2023, 685–692.

Anum Shahid – Gohar Masood Qureshi – Faiza Chaudhary: Transforming Legal Practice. The Role of AI in Modern Law. *Journal of Strategic Policy and Global Affairs*, 1/2023, 36–42.

K. Kemp – G. Baxter – J. Zeleznikow: Artificial intelligence and the legal profession. Ethical and regulatory challenges. *Law, Technology and Humans*, 1/2023, 1–18.

Ammar Zafar: Balancing the scale. Navigating ethical and practical challenges of artificial intelligence (AI) integration in legal practices. *Discover Artificial Intelligence*, 4/2024.

Meiqi Qi – Xichang Yao – Qianqian Zhu – Ge Jin: The impact and challenges of AI on the legal industry. *Journal of Artificial Intelligence Practice*, 1/2024, 64–70.

E. Briggs – K. Dyer: Understanding the implications of algorithmic opacity. *Journal of Ethics in Technology, 5*(2) 2023, 87–102.

B. Friedman: Algorithmic Negligence. Redefining Liability in the Age of Black Box AI. *Harvard Law Review,* 136(8) 2023, 2145–2189.

F. Liang – D. Greenbaum: The Public as Beta Testers. Legal Implications of Deploying Opaque AI Systems. *Yale Journal of Law and Technology,* 24(2) 2022, 312–358.

F. Doshi-Velez – Been Kim: Towards a rigorous science of interpretable machine learning. Proceedings of the 34th Conference on Neural Information Processing Systems (2022).

J. Whittlestone – A. Ovadya – M. Cinelli: The hidden dangers of AI. Strategies for uncovering latent risks in autonomous systems. *Journal of AI Safety,* 5(2) 2023, 78–95.

S. Rahman – L. Chen – T. Nguyen: Probing the unknown. Novel approaches to AI system interrogation for hazard detection. In: *Proceedings of the International Conference on AI, Ethics, and Safety*, 2024. 213-229.

L. Chen – G. K. Hadfield: The AI revolution in contract law. Implications and challenges. *Stanford Law Review*, 75(3), 2023, 621–680.

S. Goldberg: AI-proofing the law. New challenges for legal practitioners in the age of artificial intelligence. *Yale Law Journal*, 131(5), 2022, 1024–1078.

Corinne Cath: *Governing artificial intelligence: ethical, legal and technical opportunities and challenges*. Philosophical Transactions of the Royal Society A, 376(2133), 2018.0080. https://royalsocietypublishing.org/doi/full/10.1098/rsta.2018.0080.

Michael Veale – Frederik Zuiderveen Borgesius: Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 4/2021, 97–112.

Thilo Hagendorff: How AI ethics guidelines can be applied and how they can be improved. *AI and Ethics*, 2(1), 2022, 1–13.

Araz Taeihagh: Governance of artificial intelligence. A comparative analysis of national strategies. *Policy and Society*, 42(1), 2023, 156–175.

H. Müller – A. Schmidt: Implementing Trustworthy AI. A Pan-European Assessment. *Digital Policy, Regulation and Governance*, 26(3), 2024, 301–320.

M. Kowalski – A. Nowak: The Right to Explanation in Practice. Challenges and Solutions. *European Data Protection Law Review*, 10(1), 2024, 78–95.

C. Dubois – T. Van der Meer: Explainability Requirements Under the EU AI Act. A Technical and Legal Analysis. *AI and Law*, 32(2), 2024, 189–210.

THE *NE BIS IN IDEM* PRINCIPLE AND THE DMA – AFTER BPOST AND NORDZUCKER CASES

Fatma Ceren Morbel[1]

ABSZTRAKT ■ Az elmúlt néhány évben a digitális technológiák megjelenése megváltoztatta a gondolkodásmódunkat és azt, amit korábban lehetségesnek tartottunk. Mivel a digitális piacok is megváltoztak, szükség volt egy szabályozási keretre. A digitális piacokról szóló törvény ("DMA") az egyik legújabb példája az EU azon törekvéseinek, hogy tisztességes és nyitott piacokat biztosítson a digitális térben. A DMA vitát váltott ki az EUMSZ 101. és 102. cikkének a digitális platformokra való alkalmazásával kapcsolatos jelenlegi szabályokról. A DMA hatályba lépése óta és az elfogadásának folyamata során aggályok merültek fel a versenyszabályokhoz való hasonlóságával kapcsolatban. Bár a DMA és a trösztellenes jogérvényesítés kiegészítik egymást, az EU-ban a digitális platformokra többféle szabályozási keretet kell alkalmazni. Így valószínű, hogy a *ne bis in idem* elve a DMA és az uniós versenyjog párhuzamos alkalmazásaként fog érvényesülni. E tanulmány célja a *ne bis in idem* elv elemzése a DMA alapján, különös tekintettel a bpost és a Nordzucker ügyekre.

ABSTRACT ■ Over the past few years, the advent of digital technologies has changed how we think as well as what we once considered possible. As digital markets have also changed, there was a need for a regulatory framework. The Digital Markets Act ("DMA") is one of the recent examples of the EU's efforts to ensure fair and open markets in the digital realm. The DMA sparked a debate regarding the current rules regarding the application of Articles 101 and 102 TFEU to digital platforms. Since the DMA entered into force and throughout its adoption process, concerns have arisen about its similarities to competition rules. Although the DMA and antitrust enforcement are complementary, multiple regulatory frameworks will apply to digital platforms in the EU. Thus, it is likely that the *ne bis in idem* principle will arise as a parallel application of both the DMA and EU competition law. The purpose of this paper is to analyse the *ne bis in idem* principle under the DMA with a particular focus on bpost[2] and Nordzucker[3] cases.

Keywords: *ne bis in idem* principle, digital markets, Digital Markets Act, Competition Law, antitrust, duplicate proceedings

[1] PhD Student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

[2] C-117/20 *bpost* [2022]. ECLI:EU:C:2022:202.

[3] C-151/20 *Nordzucker and Others* [2022]. ECLI:EU:C:2022:203.

1. Introduction

The digital age has brought a number of benefits, including increased accessibility to information and improved communication between people around the globe. However, some concerns exist, including data theft and loss of privacy, the replacement of labour by machines, the dominance of a few ecosystems and platforms, and the reinforcement of economic inequality.[4] Competition law regulates and contributes to several benefits for consumers in order to address concerns regarding the dominance of some platforms, including reduced prices, efficiency, innovation, and more choices.[5]

The purpose of EU competition law is to ensure that businesses are treated fairly and equally, and in a level playing field, while ensuring choice and fair pricing for conditions. Although, there was also a discussion of whether the existing EU competition law was sufficient to deal with the current and changing digital word problems.

Due to the lengthy and complicated ex post enforcement procedures associated with Article 102 TFEU, it faces several challenges currently despite its broad substantive scope. Since it can cause a lack of timely intervention and the absence of effective remedies, the DMA[6] was introduced as a new ex-ante tool to complement EU competition law.[7]

Following the adoption of the Digital Services Package by the European Parliament in July 2022, the Council of the European Union adopted both the Digital Services Act and the Digital Markets Act. As of November 1, 2022, the DMA has come into effect and the DMA rules became effective in May 2023.

According to Regulation 1/2003,[8] it is possible to conduct parallel proceedings in the area of competition law.[9] In addition, since the DMA states that its application is without prejudice to the enforcement of competition law, it is

4 Jacques Crémer – Yves-Alexandre de Montjoye – Heike Schweitzer: Competition policy for the digital era. Luxembourg, Publications Office of the European Union, 2019. 2.

5 European Commission, Why is competition policy important for consumers? https://competition-policy.ec.europa.eu/about/why-competition-policy-important-consumers_en.

6 Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), Explanatory Memorandum, COM(2020) 842 final 2020/0374(COD).

7 Francesco Ducci: Gatekeepers and Platform Regulation Is the EU Moving in the Right Direction? *SciencesPo Chair Digital, Governance and Sovereignty*, 2021, 4.

8 Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.

9 Recital 22 of Regulation 1/2003; Case C-17/10, Toshiba Corporation and Others, EU:C:2012:72, paras 81 and 82.

also possible to have parallel proceedings with Article 101 and Article 102 TFEU according to the DMA.

As parallel proceedings may be pursued both under EU competition law and under the DMA, the *ne bis in idem* principle emerges, which translates from Latin as *"not twice about the same".* This principle appears in Article 50 of the Charter of Fundamental Rights and as a result, under this provision, no one shall be subject to retrial or punishment for an offense for which he or she has already been convicted or acquitted in the EU.

This paper examines the purpose of the DMA in Section II, and then describes how the ne bis in idem principle has evolved in competition law with a focus on the bpost and Nordzucker cases in Section III. Finally, Recital 86 of the DMA is discussed in relation to a potential duplication of proceedings in Section IV.

2. The purpose of the DMA

Article 114 TFEU provides the legal basis for the DMA in order to contribute to the proper functioning of the internal market by ensuring contestability and fairness for all market players in the digital sector.

The European Commission stated the purpose of the DMA as:

"The objective of the proposal is therefore to allow platforms to unlock their full potential by addressing at EU level the most salient incidences of unfair practices and weak contestability so as to allow end users and business users alike to reap the full benefits of the platform economy and the the digital economy at large, in a contestable and fair environment."[10]

It is evident from the text of the DMA that the terms contestability and fairness are used extensively. Also, it is possible to see how these terms relate to each other in the DMA as follows:

"Contestability and fairness are intertwined. The lack of, or weak, contestability for a certain service can enable a gatekeeper to engage in unfair practices. Similarly, unfair practices by a gatekeeper can reduce the possibility of business users or others to contest the gatekeeper's position. A particular obligation in this Regulation may, therefore, address both elements."[11]

Contestability is defined as the ability to overcome entry barriers, whereas fairness is defined as the ability to challenge the imbalance between the rights

[10] Proposed DMA. https://publications.europa.eu/resource/cellar/2c2bf2fb-3f85-11eb-b27b-01aa75ed71a1.0001.03/DOC_1.

[11] Recital 34, DMA.

and obligations of gatekeepers and business users by enabling the latter to benefit from innovation.[12]

As the purpose of the DMA (contestability and fairness) differs from that of the competition law (protection of undistorted competition), it is important to distinguish it from competition law implementation. The DMA's provisions are applicable without prejudice to Articles 101 and 102 TFEU. Therefore, digital platforms are subject to both Article 102 TFEU and the DMA. Accordingly, the DMA imposes obligations on gatekeepers and Article 102 TFEU imposed on dominant undertakings. Since it is possible that these two could be the same, the principle of *ne bis in idem* is invoked.

3. The evolution of the *ne bis in idem* principle in Competition Law

The *ne bis in idem* principle is based on *res judicata*, that requires that a person can not be prosecuted more than once for the same (criminal) behaviour.[13] It is a fundamental right that enshrined in Article 50 of the Charter and in Article 4 of Protocol No 7 to the ECHR.

According to Article 50 of the Charter:

"no one shall be liable to be tried or punished again in criminal proceedings for an offence for which he or she has already been finally acquitted or convicted within the Union in accordance with the law."

Therefore, under this provision, no person shall be subject to a retrial or punishment for an offense for which he or she has already been convicted or acquitted in the EU.[14] The ne bis in idem principle is not limited to proceedings described as criminal in national law, but includes administrative penalties that are criminal in nature. It is based on what is known as the Engel criteria.[15]

To decide the criminal in nature, the following criteria should be considered:[16]

[12] Christophe Carugati: The Digital Markets Act is about enabling rights, not obliging changes in market conditions, 6 September 2023. https://www.bruegel.org/analysis/digital-markets-act-about-enabling-rights-not-obliging-changes-market-conditions.

[13] Martin Wasmeier: The principle of ne bis in idem. *Revue internationale de droit pénal*, 1-2/2006 , 121–130.

[14] Hans-Jurgen Bartsch: Council of europe ne bis in idem. The european perspective. *Revue internationale de droit pénal,* 3-4/2002, 1163–1171.

[15] Judgment of the ECtHR of 8 June 1976, Engel and Others v. Netherlands (CE:ECHR:1976:0608JUD000510071).

[16] The Platform Law Blog, 'Ne bis in idem and the DMA: the CJEU's judgments in bpost and Nordzucker – Part I', 2022. https://theplatformlaw.blog/2022/03/28/ne-bis-in-idem-and-the-dma-the-cjeus-judgments-in-bpost-and-nordzucker-part-i/.

"(i) the legal classification of the offence under national law;
(ii) the intrinsic nature of the offence;
(iii) the degree of severity of the penalty which the person concerned is liable to incur."

Consequently, an administrative penalty imposed under competition law may be considered criminal.

The *ne bis in idem* principle serves both as a guarantee against the prosecution of the same individual for the same facts in multiple instances and contributes to the stability of the legal system by ensuring that judicial decisions are final.[17]

Two factors are important when determining whether the *ne bis in idem* principle has been violated: (i) *"whether a second trial or punishment is involved"* (bis condition) and (ii) *"whether the facts are the same"* (idem condition).[18]

As compared to the determination of bis condition, idem condition could be more challenging and also it raised controversy. The CJEU applied different idem criteria that can be classified as *idem factum* and *idem crimen*.

Double proceedings that fall outside of the scope of the EU competition law were assessed using an *idem factum* approach. As a result of this approach, it was only important whether the two proceedings concerned the same persons and facts, while the legal characterisation of the facts is irrelevant.[19] In this regard, the *idem factum* approach might be viewed as a broader application of the *ne bis in idem* principle. The CJEU hold this approach in Menci[20] case. In its judgment, the CJEU acknowledged that duplication of proceedings is a limitation of the right guaranteed by Article 50 of the Charter, but such a restriction may be justified on the basis of Article 52(1) of the Charter.[21]

Article 52(1) of the Charter states that any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and must respect their essence. A limitation to those rights and freedoms may be made only in accordance with Article 52(1) thereof, provided it is necessary and genuinely meets objectives of general interest recognised by the Union or the need to protect other people's rights and freedoms.[22]

17 Araceli Turmo: Ne bis in idem in European Law. A Difficult Exercise in Constitutional Pluralism. *European Papers*, 3/2020, 1341–1356. 1344.

18 Annegeret Engel – Xavier Groussot – Emilia Holmberg: The Digital Markets Act and the Principle of Ne Bis in Idem. A Revolution in the Enforcement of EU Competition Law? In: Annegret Engel – Xavier Groussot – Gunnar Thor Petursson (ed.): *New Directions in Digitalisation. Perspectives from EU Competition Law and the Charter of Fundamental Rights*. Springer, Open-Access, 2023. 187-218. 192.,

19 The Platform Law Blog 2022.

20 C-524/15 *Menci* [2018]. ECLI:EU:C:2018:197.

21 Ibid.

22 Ibid.

But on the other hand, the CJEU adopted also the *idem crimen* approach in several cases[23], that requires not only the same person and facts, but also the same protected legal interest. Since *idem factum* can be considered as a double identity of the facts, *idem crimen* can be viewed as a triple identitiy of facts that also refers to the same protected legal interest.

The principle of *ne bis in idem* has been narrowed under the *idem crimen* approach.

Depending on the field of EU law in which it was applied, the *ne bis in idem* principle has been implemented differently. Although the CJEU had adopted a broad view of *ne bis in idem* in all other areas of EU law, it had adopted a narrow view in the area of EU competition law, consequently, it sparked controversy and criticism.

In March 2022, the CJEU ended this controversy with its two judgments, bpost and Nordzucker.

A postal services provider in Belgium, bpost, adopted a new tariff system in 2010 which the Postal Regulator found to be discriminatory in relation to tariff rules. After that, in July 2011, bpost was fined by the postal regulator.

The Court of Appeal of Brussels annulled the decision and the judgment was subsequently rendered final. At this time, the Belgian Competition Authority ruled that bpost had abused its dominant position in breach of Article 102 TFEU by implementing the new tariffs and imposed a fine.

In its appeal, bpost argued that the decision of the Belgian Competition Authority was incompatible with the *ne bis in idem* principle, since it was based on the same tariff system for which the Belgian postal regulator had already fined it. In contrast, the Authority claimed that each decision was adopted in accordance with a variety of rules protecting different legal interests, therefore, the *ne bis in idem* principle was not applicable. It was referred to the CJEU for a preliminary ruling following an appeal process.

As a first step, the CJEU recognised that Article 50 of the Charter contains the *ne bis in idem* principle as a fundamental principle of EU law, that is also enshrined in the ECHR.[24] Consequently, it assessed the criminal nature of both sets of proceedings and concluded that they were criminal in nature.[25]

The CJEU found that the bis criteria were satisfied, as the judgement on annulment of the Postal Regulator's decision had become final.[26]

[23] C-204/00 *P Aalborg Portland and Others v Commission* [2004] ECLI:EU:C:2004:6, C-17/10 *Toshiba Corporation e.a* [2012] ECLI:EU:C:2012:72, C-857/19 *Slovak Telekom* [2021] ECLI:EU:C:2021:139.

[24] C-117/20 *bpost* [2022] paras. 22-23. ECLI:EU:C:2022:202.

[25] Ibid.

[26] Ibid.

Regarding the idem criteria, according to the CJEU, the two sets of proceedings at issue in the main action are directed against the same legal person, bpost.[27] Also, it was stated that *"the relevant criterion for the purposes of assessing the existence of the same offence is identity of the material facts, understood as the existence of a set of concrete circumstances which are inextricably linked together and which have resulted in the final acquittal or conviction of the person concerned."* and the legal classification of the facts under national law and the legal interest protected are irrelevant.[28] Therefore, it adopted idem factum approach.

As part of its evaluation, the CJEU examined whether a limitation of the *ne bis in idem* is justified by Article 52(1) of the Charter. In accordance with Article 52(1) of the Charter, a limitation may be justified if it is provided by law and respects the essence of the rights and freedoms as well as the principle of proportionality.[29]

Accordingly, the CJEU concluded that, the listed factors are met:[30]

"Article 50 of the Charter, read in conjunction with Article 52(1) thereof, must be interpreted as not precluding a legal person from being fined for an infringement of EU competition law where, on the same facts, that person has already been the subject of a final decision following proceedings relating to an infringement of sectoral rules concerning the liberalisation of the relevant market."

In the Nordzucker case, the undertaking filed leniency applications to the German and Austrian Competition Authorities by disclosing a cartel between Nordzucker and two other sugar producers. In 2010, the Austrian Competition Authority filed an action declaring Nordzucker and Südzucker to be in violation of Article 101 TFEU. A telephone conversation between the sales directors of Nordzucker and Südzucker was used as evidence.[31]

The German Competition Authority concluded in September 2014 that Nordzucker and Südzucker violated Article 101 TFEU and German law. The German Authority also referred to the content of the phone call, which was the only Austrian market-related fact.[32]

As the phone call used as evidence by the Austrian Authority had already been subject to another penalty, the Austrian Court dismissed the action brought by the Authority on the grounds that imposing a penalty would violate the principle of *ne bis in idem*. In response to the judgment, the Authority appealed

27 Ibid.
28 Ibid.
29 Ibid.
30 Ibid.
31 C-151/20 *Nordzucker and Others* [2022] paras. 14-16.ECLI:EU:C:2022:203.
32 Ibid.

to the Supreme Court of Austria, which requested that the CJEU render a preliminary ruling.[33]

Briefly, the CJEU decided that proceedings initiated by two national competition authorities to prohibit anticompetitive agreements are meant to pursue the same legal interest. Moreover, the CJEU stated that a duplication of proceedings and penalties that do not pursue complementary aims relating to different aspects of the same conduct cannot be justified under Article 52(1) of the Charter, and it might be justified if their aims are complementary.[34]

4. Recital 86 of the DMA and the consideration of a duplication in proceedings

Recital 86 of the DMA explains how the ne bis in idem principle is implemented: *"The Commission and the relevant national authorities should coordinate their enforcement efforts in order to ensure that those principles are respected. In particular, the Commission should take into account any fines and penalties imposed on the same legal person for the same facts through a final decision in proceedings relating to an infringement of other Union or national rules, so as to ensure that the overall fines and penalties imposed correspond to the seriousness of the infringements committed."*

Recital 86 is intended to facilitate the cooperation between the Commission and National Competition Authorities (NCAs). However, this provision remains problematic since it is possible to pursue parallel proceedings under both the DMA and competition law against the same undertaking as long as the duplication is complementary. While it is likely that the Commission would prefer to impose fines and remedies under the DMA as opposed to pursuing the longer route of enforcing competition law, NCAs can also apply competition law to conduct that has already been subject to DMA enforcement. Under Article 102 TFEU, NCAs may seek to achieve more ambitious results than the Commission achieved under the DMA.[35] Gatekeepers may be deprived of *ne bis in idem* protection since the Commission views the DMA as complementary to EU competition law. Thus, the duplication of sanctions and remedies may result in an increased burden on gatekeepers and a fragmentation risk.

[33] The Platform Law Blog 2022.

[34] Engel et al. 2023.

[35] Giorgio Monti: The Digital Markets Act – Institutional Design and Suggestions for Improvement. *TILEC Discussion Paper*, 4/2021. 15.

5. Conclusion

As a result of the bpost and Nordzucker judgments, the EU's approach to *ne bis in idem* has been further clarified. In brief, the Court adopted a broad interpretation of idem based on the identity of the offender and the facts, stressing the importance of proportionality.

In this approach, a balance is sought between the protection of Article 50 of the Charter and the effective enforcement of administrative regulations. Consequently, it is possible to duplicate proceedings under the DMA and EU competition law as well as national law against the same undertaking and based on the same facts, provided that the duplication serves complementary aims and follows proportionality principles. However, since the duplication of proceedings may increase the burden on gatekeepers, there needs to be more clarity in this area.

Bibliography

Articles

Hans-Jurgen Bartsch: Council of europe ne bis in idem. The european perspective. *Revue internationale de droit pénal,* 3-4/2002, 1163–1171.

Jacques Crémer – Yves-Alexandre de Montjoye – Heike Schweitzer: Competition policy for the digital era. Luxembourg, Publications Office of the European Union, 2019.

Francesco Ducci: Gatekeepers and Platform Regulation Is the EU Moving in the Right Direction? *SciencesPo Chair Digital, Governance and Sovereignty*, 2021.

Annegeret Engel – Xavier Groussot – Emilia Holmberg: The Digital Markets Act and the Principle of Ne Bis in Idem. A Revolution in the Enforcement of EU Competition Law? In: Annegret Engel – Xavier Groussot – Gunnar Thor Petursson (ed.): *New Directions in Digitalisation. Perspectives from EU Competition Law and the Charter of Fundamental Rights*. Springer, Open-Access, 2023. 187-218.

Giorgio Monti: The Digital Markets Act – Institutional Design and Suggestions for Improvement. *TILEC Discussion Paper,* 4/2021.

Araceli Turmo: Ne bis in idem in European Law. A Difficult Exercise in Constitutional Pluralism. *European Papers*, 3/2020, 1341–1356.

Martin Wasmeier: The principle of ne bis in idem. *Revue internationale de droit pénal*, 1-2/2006, 121–130.

Cases
C-117/20 *bpost* [2022].
ECLI:EU:C:2022:202.
C-151/20 *Nordzucker and Others* [2022].
ECLI:EU:C:2022:203.
C-524/15 *Menci* [2018].
ECLI:EU:C:2018:197.
C-204/00 *P Aalborg Portland and Others v Commission* [2004] ECLI:EU:C:2004:6.
C-17/10 *Toshiba Corporation e.a* [2012] ECLI:EU:C:2012:72.
C-857/19 *Slovak Telekom* [2021] ECLI:EU:C:2021:139.
Judgment of the ECtHR of 8 June 1976, Engel and Others v. Netherlands (CE:ECHR:1976:0608JUD000510071).

Regulations
Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.
Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), Explanatory Memorandum, COM(2020) 842 final 2020/0374(COD).

Internet Resources
Christophe Carugati: The Digital Markets Act is about enabling rights, not obliging changes in market conditions, 6 September 2023. https://www.bruegel.org/analysis/digital-markets-act-about-enabling-rights-not-obliging-changes-market-conditions.
European Commission, Why is competition policy important for consumers?, https://competition-policy.ec.europa.eu/about/why-competition-policy-important-consumers_en.
The Platform Law Blog, 'Ne bis in idem and the DMA: the CJEU's judgments in bpost and Nordzucker – Part I', 2022. https://theplatformlaw.blog/2022/03/28/ne-bis-in-idem-and-the-dma-the-cjeus-judgments-in-bpost-and-nordzucker-part-i/.

CHALLENGES IN THE LEGAL FRAMEWORK FOR UTILIZING ELECTRONIC EVIDENCE IN CYBER-CRIME IN RWANDA

Francois Regis Nshimiyimana[1]

ABSZTRAKT ■ Ez a tanulmány a Ruandában jelentkező azon kihívásokkal foglalkozik, amelyek az elektronikus bizonyítékok hatékony felhasználásával kapcsolatosak a kiberbűnözés elleni küzdelemben, ami , ami kulcsfontosságú a mai digitális korban. Fejlődő országként Ruanda akadályokba ütközik az elektronikus bizonyítékok jogrendszerébe való integrálása terén, ami akadályozza a kiberfenyegetések hatékony leküzdését. A tanulmány jogi és technikai szempontból vizsgálja ezeket az akadályokat, azzal a céllal, hogy megértse hatásukat Ruanda kiberbűnözés elleni erőfeszítéseire.A feltárt kulcskérdések a következők: milyen jogi keretbeli kihívások akadályozzák az elektronikus bizonyítékok hatékony felhasználását a kiberbűnözési ügyekben Ruandában? Léteznek-e Ruandán belül stratégiák vagy jogi reformok ezen akadályok leküzdésére? Hogyan segíthetnek a legjobb nemzetközi gyakorlatokból származó tapasztalatok a kiberbűnözési ügyekben alkalmazott elektronikus bizonyítékokkal kapcsolatos ruandai jogi keret lehetséges megoldásaiban? A kutatási módszertanmagában foglalja a jogi keretekre, kiberbűnözésre és elektronikus bizonyítékokra vonatkozó szakirodalom mélyreható áttekintését,, valamint a vonatkozó ruandai jogszabályok és politikák elemzését. A tanulmány zárásként potenciális megoldásokat javasol Ruanda jogrendszere hatékonyságának növelésére a kiberfenyegetések elektronikus bizonyítékok felhasználásán keresztül történő leküzdésében.

ABSTRACT ■ This paper delves into Rwanda's challenges in effectively utilizing electronic evidence to combat cybercrimes, a critical need in today's digital era. As a developing nation, Rwanda faces hurdles in integrating electronic evidence into its legal system, hindering its ability to tackle cyber threats efficiently. The paper examines these obstacles from legal and technical perspectives, aiming to understand their impact on Rwanda's cybercrime efforts. Key questions explored include: What legal framework challenges impede the effective use of electronic evidence in cybercrime cases in Rwanda? Are there existing strategies or legal reforms within Rwanda to address these obstacles? How can insights from international best practices inform potential solutions for Rwanda's legal framework regarding electronic evidence in cybercrime cases? The research methodology involves an in-depth review of the literature on legal frameworks, cybercrimes, and electronic evidence, coupled with an

[1] PhD student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

analysis of relevant Rwandan laws and policies. The paper concludes by proposing potential solutions to enhance Rwanda's legal system's effectiveness in combating cyber threats through electronic evidence.

Keywords: electronic evidence, cyber-crime

1. Introduction

Cybercrime, including in Rwanda, has become a significant problem everywhere in the digital era. The techniques employed by cybercriminals to perpetrate crimes also evolve along with technology. The legal framework for using electronic evidence is essential to guarantee successful prosecution and justice in cybercrime situations. Due to the difficulties in obtaining, maintaining, and presenting electronic evidence within its judicial system, Rwanda, like many other nations, needs help. That is why Rwanda felt an obligation to join the Convention on Cybercrime and its additional Protocol concerning the criminalization of acts of racist and xenophobic nature committed through computer systems[2]. It has made significant strides in addressing cybercrime and enhancing its legal framework to accommodate electronic evidence. However, challenges persist in effectively utilizing electronic evidence in cybercrime cases.

1.1. Background and development of electronic evidence in cybercrime in Rwanda

The evolution of electronic evidence in Rwanda began in the early 2000s, coinciding with an increase in cyber-related crimes in the country. In response to this trend, the Rwanda Information and Communication Technology Authority (RITC) was established in 2002 to oversee the information and communication technology sector.[3] This year marked the initiation of Rwanda's efforts to incorporate electronic evidence into cybercrime investigations.

[2] The Convention on Cyber Crime, done in Budapest, Hungary, on November 21, 2001, and its additional Protocol concerning the criminalization of acts of racist and xenophobic nature committed through computer systems, done in Strasbourg, France, on January 28, 2023.

[3] Ronald Serwanga: *Legal mechanisms for enforcing electronic transactions in Rwanda. Diss.* University of Rwanda, 2019. 8-9.

In 2007, the Rwanda National Police (RNP) established its Cyber Crime Unit to investigate and prosecute cybercrime cases[4]. This unit has played a crucial role in integrating electronic evidence into Rwanda's justice system by training officers to handle digital evidence and fostering collaboration with international partners to exchange best practices.

1.2. Definition of cyber-crime and its increasing prevalence

Any illegal behavior involving a computer, networked device, or network is cyber-crime[5]. While most cyber-crimes are committed to making money for the perpetrators, some are explicitly committed to harming or destroying computers or other devices. Others disseminate viruses, illicit information, photographs, and other items via computers or networks. Certain cyber-crimes combine the two tactics of targeting computers and infecting them with a virus that spreads to different devices and, occasionally, even entire networks.

One of cybercrimes' main consequences is their financial impact. Cybercriminal activities often aim for monetary gain and can encompass various profit-motivated offenses.[6] These can range from ransomware attacks and internet scams to identity theft and efforts to pilfer financial account details, credit cards, or other payment card information.

1.3. Significance of electronic evidence in combating cyber crimes

Electronic evidence in cybercrime cases pertains to data stored, transmitted, or accessed on digital devices and networks, represented in binary code. This type of evidence holds significant importance in legal proceedings, as it can be used to construct a case against a defendant and presented in court. Similar to how physical evidence, such as fingerprints or DNA, can link a person to a crime, digital evidence provides insight into activities, interactions, and intentions. Much like physical evidence can create a timeline of events in a crime; digital

4 Bernard Walumoli: *A Critical Analysis of the Challenges Facing Countercybercrime in 21st Century Africa: a Focused Comparison of Kenya and Rwanda. Diss*. University of Nairobi, 2021. 53-77.

5 Brian Payne: Defining cybercrime. In: Thomas J. Holt – Adam M. Bossler (eds.): *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* Cham, Springer, 2020. 3-25. https://link.springer.com/referencework/10.1007/978-3-319-78440-3.

6 Ki Hong Steve Chon: *Cybercrime precursors. Towards a model of offender resources. Doctor of Philosophy dissertation*. Australian National University, 2016. 20.

evidence serves a similar purpose in the virtual world.[7] It helps create a narrative of what occurred, why, and how it unfolded.

Similar to how physical evidence, such as fingerprints or DNA, assists in understanding the sequence of events in a crime, digital evidence serves a similar function in the digital domain. It aids in creating a narrative of the events, motivations, and actions that are believed to have occurred. By gathering and examining digital evidence, legal experts can reconstruct timelines, validate assertions, and potentially reveal discrepancies or omissions in the Prosecution's argument. Thus, grasping the intricacies of digital evidence and its significance is crucial for legal professionals and individuals accused of cyber-crime.

2. Current legal provisions on electronic evidence and cyber crime under Rwandan law

The spread of the Internet has been the most significant social and technological change in recent times, reducing trade barriers and playing a considerable role in supporting sustainable development in Rwanda. However, our increased dependence on the Internet and digital technologies increases our vulnerability to cyber threats, and our increasing reliance on cyberspace has brought new risks; criminals are increasingly using cyber-space to gain access to personal information, steal businesses and intellectual property, and gain knowledge of sensitive government-held information for financial or political gain or other malicious purposes.

Rwanda's legal framework for handling electronic evidence is primarily governed by Law n°68/2018 of 30/08/2018 on Electronic Messages, Electronic Signatures, and Electronic Transactions. While this Law provides a foundation for dealing with electronic evidence, its application to cybercrime cases presents complexities that must be addressed. The Law outlines provisions related to electronic signatures, messages, and transactions but lacks specific guidelines on the admissibility and authenticity of electronic evidence in criminal proceedings. The government of Rwanda established Law n°60/2018 of 22/8/2018 on the prevention and punishment of cybercrimes; it aims to prevent and punish cyber-crimes.[8] Regarding electronic evidence, the same law states, *"If the person holding*

[7] Lars Daniel: Digital Forensics—What Exactly Is Digital Evidence? *Forbes*, November 17, 2024, 04:11 PM EST. Updated November 17, 2024, 05:29 PM EST, https://www.forbes.com/sites/larsdaniel/2024/11/17/what-exactly-is-digital-evidence/.

[8] Article 1 of the Law n°60/2018 of 22/8/2018 on prevention and punishment of cybercrimes, Official Gazette n°Special of 25/09/2018.

data or the evidential value of data is not willing to cooperate in disclosure or preservation of data, the prosecution authority may seek a court order compelling such person to do so." In terms of authorization to employ a forensic method, the law also stipulates that: *"if the prosecution authority has reasonable grounds to believe that essential evidence cannot be collected without the use of the scientific method, it may request the court to order for the use of a forensic method. The order is valid for thirty days. Upon application made by the organ in charge of Prosecution, the court may extend that period for a further period of thirty days or to such other period as it considers necessary".*

Rwanda also established law n°24/2016 of 18/06/2016 governing information and communication technologies, which aims to develop a framework of Information and Communication Technologies (ICT) policy and regulation, with emphasis on promoting national Information and Communication Technologies policy objectives, establishing a licensing and regulatory framework in support of national policy objectives for the Information and Communication Technologies industry taking into account the convergence of technologies; establishing and strengthen the relevant institutions by providing them with the powers and procedures that are necessary for the implementation; establishing Rwanda as a major global center and hub for communications and multimedia information; promoting an information society for the enhancement of quality of both life and work and ensuring an equitable provision of affordable services over ubiquitous national infrastructure.[9]

Concerning the admissibility and evidential weight of electronic records, the same law in Article 14 states that: *"in any legal proceedings, an electronic record has admissibility and evidential value."* In terms of the admissibility of an electronic signature, the above-mentioned law in Article 146 states that: *"where it is required to have a signature of a person on an electronic record, an electronic signature has admissibility and evidential value in any legal proceedings if the method used indicates the originator of the record and that the originator approves the information contained in the record, and that method is reliable for the purpose for which the electronic record was generated or communicated, in the light of agreement."*

The law n°24/2016 of 18/06/2016 governing information and communication technologies aligns with *"the principle of equivalence"*, asserting that electronic evidence, encompassing emails, digital documents, social media posts, and various digital communications, should be treated on par with traditional forms of evidence like physical documents or witness testimony[10]. It emphasizes that

[9] Article 1 of the Law n°24/2016 of 18/06/2016 governing information and communication technologies, Official Gazette n°26 of 27/06/2016.

[10] Bradley Lawrence Schatz: *Digital evidence, representation, and assurance. Diss*. Queensland University of Technology, 2007. 30-32.

courts and legal systems should not unfairly disregard or dismiss electronic evidence solely based on its digital format.

3. Challenges in the legal framework for utilizing electronic evidence in cyber-crime in Rwanda

In the past two decades, a significant increase in interest in cyber crime has led to a substantial body of literature. However, there are notable gaps in this existing knowledge. For instance, there is a need for more accurate and valid data on the frequency, characteristics, and patterns of cyber-crime. Additionally, there is a lack of research on effective strategies for combating and preventing cybercrime[11]. In Rwanda, using electronic evidence in cyber crime cases presents various legal challenges. These challenges encompass legal, technical, privacy, and data protection aspects that must be carefully addressed to handle cyber-crime incidents effectively.

3.1. Legal challenges

Electronic evidence collection, admissibility, and authenticity in cybercrime cases present significant challenges. Matters such as the admissibility of digital evidence, chain of custody requirements, and ensuring compliance with international standards for electronic evidence are notable hurdles. The recent increase in cyber-crime has highlighted the critical importance of preserving electronic evidence, especially in countries like Rwanda, where legal frameworks must be adjusted to the digital era.

3.1.1. Issue relating to cyber-crime definition

Cyber-crime has yet to receive a unanimous definition, both nationally and internationally.[12] This lack of consensus on the concept originates from a myriad of definitions proposed on all sides by states and official international organizations, which confront several interests and systems. Classically, these definitions limit cyber-crime to the modus operandi of the cyber-offenders or the object of the

[11] Fawn T. Ngo – K. Jaishankar: Commemorating a Decade in Existence of the International Journal of Cyber Criminology. A Research Agenda to Advance the Scholarship on Cyber Crime. *International Journal of Cyber Criminology*, 1/2017, 4-5.

[12] Charlie Plumb: Understanding the UN's New International Treaty to Fight Cybercrime. UN CPR, July 30, 2024. Available at: https://unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime.

offense. This is the case, among others, according to the framework established by the Organization for Economic Cooperation and Development (OECD), which, alluding to the processing or security of data, adopts cyber-crime as any unlawful, unethical, or unauthorized conduct relating to automatic data processing and data transmission.[13] Similarly, the United Nations also limits cyber-crime to attacks on the security of computer systems. Other definitions, particularly those of the United Kingdom are limited solely to fraudulent access to a computer system, which undoubtedly excludes a significant part of the offense spectrum of cybercrime, namely, all offenses that can be committed through a system.[14] In Rwanda, cyber-crime is not defined in the Penal Code, Criminal Procedure, or any other legal text, regardless of the fact that Law n°60/2018 of 22/8/2018 on prevention and punishment of cyber crimes mentions this term from start to finish.[15]

3.1.2.

Lack of legal provision on cybercrime under Rwandan Law relating to evidence and its productionRwandan Law n°15/2004 of 12/06/2004 relating to evidence and its production lacks a specific provision addressing electronic evidence under the Evidence and its Production Law of 2004. This Law applies to common offenses and cyber-crimes and does not explicitly cover electronic evidence. By recognizing this gap, an ongoing project has been started to revise the Law to incorporate provisions specifically addressing cyber-crimes. As we know, an electronic record has admissibility and probative value in any legal matter. An original electronic record is required to prove its content unless otherwise provided.

The requirement to produce the original electronic record is satisfied if the integrity of the electronic record system by or in which the electronic record was recorded or stored is proved or the integrity of an electronic record is proved or presumed. Under the current evidence law, an electronic record has no presumption of integrity.[16] At the same time, the competent organ may presume the integrity of an electronic record if the electronic record remains complete and unaltered except for the addition of any endorsement or any immaterial change that arises in the ordinary course of communication, storage, or display; the electronic record was certified or has been electronically signed by use of the

[13] OECD, Computer-Related Criminality. Analysis of Legal Politics in the OECD Area. 1986.

[14] Jacques Kabano – Jean Habarurema: Procedural Aspects of Cyber Crimes Investigations in Rwanda. A Comparative Study. *Makerere Law Journal*, 5/2023, 240–266.

[15] Law n°60/2018 of 22/8/2018 on Prevention and Punishment of Cyber Crimes, Official Gazette n° Special of 25/09/2018.

[16] Uniform Electronic Evidence Act 15A-1 (1998). Proceedings at page 77. https://ulcc-chlc.ca/ULCC/media/EN-Uniform-Acts/Uniform-Electronic-Evidence-Act_2.pdf.

method specified by an accredited certification entity; the integrity and content of the electronic record were notarized; the electronic record was recorded in a non-rewritable storage device or any other electronic means that do not allow alteration of the electronic records; the electronic record was examined and its integrity confirmed by an expert.

3.1.3. Lack of a comprehensive legislative framework to deal with electronic evidence

Rwanda grapples with a significant legal challenge due to a need for a comprehensive legislative framework tailored for electronic evidence in cyber-crime. Existing laws need to be updated, or there needs to be more specificity for addressing the complexities associated with cyber-crime and electronic evidence preservation. This gap can lead to confusion among law enforcement, judges, and other stakeholders as they navigate the intricacies of digital evidence. Jurisdictional issues pose another legal challenge.

3.1.4. Jurisdictional issues

Like many other nations, Rwanda grapples with the jurisdictional aspect of electronic evidence. This challenge is exemplified by the "Rwanda genocide trials", where electronic evidence played a pivotal role.

During the trials related to the 1994 Rwandan genocide, electronic evidence, including emails, digital photographs, and online communications, became crucial for establishing facts and prosecuting the perpetrators.[17] However, challenges emerged regarding jurisdiction when some of this electronic evidence was stored on servers outside Rwanda. This situation prompted questions about which legal framework should be applied to obtain and authenticate such evidence in Rwandan courts.

The jurisdictional challenge was compounded by the diversity of laws and regulations in different countries concerning the collection and admissibility of electronic evidence. Within the framework of Rwandan cyber Law, this case underscored the necessity for explicit guidelines on navigating jurisdictional issues when dealing with electronic evidence that extends beyond national borders.

3.1.5. Cross-border data access and sharing

In today's digital age, it is difficult to envision a criminal investigation that does not rely on digital evidence, considering that most of the world's information

[17] Allan Thompson (ed.): *The Media and the Rwanda Genocide*. London, Pluto Press, 2007. https://doi.org/10.2307/j.ctt18fs550.

is now stored in digital format.[18] Modern criminal evidence is not confined to digital formats; it also challenges traditional ideas of geographical boundaries and territorial jurisdiction.[19] Due to its international scope and intricate nature, cyber-crime poses substantial challenges that are hard for individual states to tackle independently[20]. With the widespread adoption of cloud computing, local storage in end-user devices has been replaced by remote storage. Consequently, data previously stored locally and accessible through domestic procedures is now frequently held by private companies and stored in jurisdictions beyond the investigating country's reach.

The process of seeking evidence across borders and dealing with jurisdictional limits in law enforcement is not recent. Governments have long established formal and informal cooperative arrangements to exchange evidence across borders while respecting each nation's territorial sovereignty. The Mutual Legal Assistance Treaty (MLAT) system, which relies on agreements between countries, sets out a formal procedure where one country can request assistance from another country to obtain evidence within its jurisdiction.[21]

The problem is that the advent of the Internet, particularly cloud computing, has disrupted the functioning of such a system of cross-border legal cooperation. As cross-border access to electronic evidence becomes familiar, it creates a unique jurisdictional conflict, as described by Andrew K. Woods. This situation arises when a criminal investigation typically confined to domestic borders now requires international cooperation.[22] Even in cases where the criminal investigation involves local suspects and victims, and the data belong to a citizen of the investigating country, authorities might still need diplomatic channels for cross-border legal cooperation.

[18] European Commission. *"Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying down Harmonized Rules on the Appointment of Legal Representatives to Gather Evidence in Criminal Proceedings." COM(2018) 225 Final - COM(2018) 226 Final - SWD(2018) 119 Final*, 14. Brussels: European Commission, 2018.

[19] IAPP. "The Globalization of Criminal Evidence." *International Association of Privacy Professionals*, 16 October 2018. https://iapp.org/news/a/the-globalization-of-criminal-evidence.

[20] Ikenga K. E. Oraegbunam: Jurisdictional Challenges in Fighting Cybercrimes. Any Panacea from International Law. *Nigerian Journal of International Law and Jurisprudence*, 6/2015, 57–65.

[21] Council of Europe: Convention on Cybercrime of the Council of Europe, opened for signature on November 23, 2001, in Budapest, Hungary, Council of Europe Treaty Series - No. 185.

[22] Jonah Force Hill – Matthew Noyes: *Rethinking Data, Geography, and Jurisdiction. Towards A Common Framework for Harmonizing Global Data Flow Controls*. New America and Cybersecurity Initiative, 2018. 32.

Rwanda has witnessed a surge in cyber-crime, which encompasses fraud, identity theft, and cyberstalking. Effectively combating these offenses requires law enforcement agencies to obtain electronic evidence stored internationally.[23] However, a cohesive legal framework for cross-border data access and sharing complicates this process. As discussed earlier, Rwanda has enacted several laws and regulations to tackle cyber-crime, offering a legal foundation for managing electronic evidence in criminal investigations and legal proceedings. Despite these measures, challenges emerge when accessing data in different jurisdictions. Infact, when the electronic evidence, vital to the investigation, is located on servers outside of Rwanda, that require collaboration and legal assistance from authorities in other jurisdictions. Obtaining and ensuring the admissibility of this evidence in Rwandan courts posed challenges due to differences in legal frameworks, data protection laws, and jurisdictional issues.

3.2. Technical challenges

Utilizing electronic evidence in cyber-crimes presents several technical challenges in Rwanda. These challenges arise from various factors, including the dynamic nature of technology, the necessity for specialized expertise, and the intricate nature of digital forensics.

3.2.1. Shortage of specialized equipment and expertise

Technical hurdles in preserving electronic evidence in developping countries like Rwanda arise from the shortage of specialized equipment and expertise. Law enforcement officers and forensic experts need more training and resources to handle and analyze digital evidence effectively.[24] This deficiency increases the risk of losing or contaminating critical evidence, potentially compromising case outcomes. The rapidly evolving nature of technology presents another technical challenge. The emergence of new devices and platforms provides cyber-criminals with new areas to exploit. This constant evolution makes it challenging for

[23] Minijust. "Law Enforcement Agencies Must Step Up by Enhancing Measures to Detect and Prevent the Cyber-Attacks from the Source." *9th Africa Working Group Meeting on Cybercrime for Heads of Units*, Kigali, Rwanda. https://www.minijust.gov.rw/news-detail/law-enforcement-agencies-must-step-up-by-enhancing-measures-to-detect-and-prevent-the-cyber-attacks-from-the-source.

[24] Scott H. Belshaw: Next Generation of Evidence Collecting. The Need for Digital Forensics in Criminal Justice Education. *Journal of Cybersecurity Education, Research and Practice*, 1/2019. https://files.eric.ed.gov/fulltext/EJ1341743.pdf.

Rwandan authorities to stay abreast of the latest cyber-crime trends and develop effective methods to preserve electronic evidence.

According to Wiles, ninety-seven percent of all high-tech crimes are estimated to go undetected[25]. It is not surprising, then, that officers assigned to investigate must possess specific knowledge and skills. Meyer and Short have proposed a job description for the ideal computer crime investigator.[26] The officer chosen to investigate computer crime should be an experienced, competent investigator with the ability to think analytically and a complete understanding of computer fraud-related laws and their application. The investigator should receive advanced training in computer crime investigation and be familiar with major operating systems. This investigator should develop professional contacts that would assist in conducting investigations.

The rapid advancements in technology and the evolving tactics of cyber-criminals necessitate that law enforcement agencies continuously update their technical tools and software, maintain current skills, conduct ongoing research, and develop effective countermeasures. Successfully investigating and prosecuting cybercrime requires individuals equipped with specialized skills and tools. However, the U.S. Government Accountability Office (GAO) has noted that the pool of qualified candidates remains limited.[27] Professionals tasked with investigating or examining cybercrime must possess unique law enforcement expertise and technical skills, including proficiency with various IT hardware, software, and forensic tools.[28] This talent scarcity creates significant challenges in recruiting such individuals, retaining them amidst competitive offers, and ensuring they remain updated on evolving technologies and increasingly sophisticated criminal techniques.

Additionally, the available technological infrastructure heavily influences the efficiency of employing electronic evidence in cybercrime investigations. In Rwanda, the lack of advanced technological infrastructure characterized by outdated or restricted forensic tools and software can impede the retrieval and analysis of electronic evidence from diverse devices. Enhancing capacity through targeted training and skill-building initiatives is essential to address

[25] Roger Wiles: *High-Tech Crime and Its Detection. A Comprehensive Study.* Cybersecurity Press, 2020, 189-230.

[26] John Franklin Meyer – Charles Short: Investigating Computer Crime. *Police Chief*, 5/1998, 28–35.

[27] United States Government Accountability Office. *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats.* Report to Congressional Requesters, GAO-07-705, June 2007. Accessed on December 28, 2024. https://www.gao.gov/assets/gao-07-705.pdf.

[28] Cyber Talents. "Cybercrime Investigation Tools and Techniques You Must Know". *Cyber Talents Blog.* Accessed December 28, 2024. https://cybertalents.com/blog/cyber-crime-investigation.

these challenges. Training programs must equip law enforcement personnel with the expertise required to adapt to technological advancements and effectively manage the complexities of modern cybercrime investigations.

3.2.2. Challenges relating to identifying electronic forgery

Electronic forgery is a notable technical challenge in Rwanda's use of electronic evidence. As the country experiences a surge in reliance on electronic evidence in legal matters, especially those related to cyber-crime and fraud, the detection of electronic forgery emerges as an intricate technical obstacle.[29] Addressing this challenge is imperative to upholding the credibility and admissibility of electronic evidence in Rwandan legal proceedings.

Detecting electronic forgery poses a significant challenge due to the advanced digital manipulation techniques available to perpetrators. The complexity of modern technology has made it more difficult to distinguish between authentic and falsified electronics. Perpetrators can access various tools to precisely alter digital documents, images, videos, and other electronic data. This complexity hinders law enforcement agencies and legal professionals from reliably detecting and proving instances of electronic forgery beyond a reasonable doubt.

An exciting email forgery occurred in the National Bank of Rwanda (NBR) when the Rwanda National Police ordered the reimbursement of the command of the uniform worn (of Rwanda Police personnel). The National Police forwarded an order of payment (ordre de payment n°0701/0750/O.P./13) to the NBR of 477.264 American dollars, which should be transferred to account n°0169-FT0517-050 of Indusind Bank in New Delhi to pay Alps International Exports (vendor). The NBR personnel in charge of the transfer received misleading information from the counterfeit email of the Alps International Exports director (rajsab992002@yahoo.com), who said that the account that should have been used in the money transfer changed to account n°0288000260017022 of DBS Bank in Singapore.

This forged email rajsab99202@yahoo.com of the criminal group called Enjreni Trading Ltd is confusing because it looks like the real email rajsab992002@yahoo.com of the director of Alps International Exports; the only difference is the "0", which has been placed before the number two. From this forged email message, the money was transferred via the account of the criminals said above, and after that, the real businessman (vendor) claimed that he did not receive the money.[30]

[29] Bernard Walumoli: *A Critical Analysis of the Challenges Facing Countercybercrime in 21st Century Africa: a Focused Comparison of Kenya and Rwanda. Diss*. University of Nairobi, 2021. 35-40.

[30] Nyarugenge Intermediate Court: Judgment in the case of Prosecution of Rwanda vs Bamporiki et al., Case No. RP 0527/13/TGI/NYGE of April 30, 2015.

It is a well-known fact that even if law enforcement agencies have done an excellent job investigating cyber-crime, at the litigation stage, the expertise of prosecution attorneys is still significant to secure the conviction of cyber criminals as it is incumbent on the Prosecution to prove his case beyond doubts; unfortunately, this is not the case as there is a dearth of savvy prosecutors in government justice departments.[31]

3.3. Privacy and data protection challenge

Balancing the need to access digital information while protecting individuals' privacy rights is a delicate matter that requires explicit legal provisions and safeguards. In Rwanda, safeguarding privacy and data is a fundamental right embedded in the nation's legal framework. The constitution of Rwanda, particularly in Article 23, explicitly ensures the right to privacy, proclaiming that *"The privacy of the home and correspondences is inviolable."* Moreover, Rwanda has implemented specific legislation, including Law N°30/2013 of 24/05/2013, that protects personal data.

While Rwanda prioritizes protecting privacy and personal data, challenges arise in obtaining and utilizing electronic evidence in cyber-crime cases. Due to the constraints imposed by privacy laws and data protection regulations, law enforcement agencies and judicial authorities may frequently confront hurdles in accessing electronic evidence. This becomes especially pertinent when evidence is stored on private devices or servers, potentially violating individuals' privacy rights.

The case of Nsabimana Callixte alias Sankara et al. vs. the Prosecution[32] has brought attention to the challenges of obtaining electronic evidence in cyber-crime cases in Rwanda. This particular case has sparked discussions regarding the adequacy of the legal framework that governs the acquisition and utilization of electronic evidence, along with concerns about the capabilities of law enforcement agencies to conduct effective investigations into cyber-crime incidents. Furthermore, the case underscores the crucial need to enhance Rwanda's legal framework by tailoring it to address cybercrime specifically and the collection of electronic evidence. This involves the formulation of comprehensive legislation, providing training and capacity-building programs for law enforcement and

[31] Peter A. Joy: Prosecution Clinics. Dealing with Professional Role. *Mississippi Law Journal*, 4/2005, 955–981. 955. https://heinonline.org/HOL/LandingPage?handle=hein.journals/mislj74&div=40&id=&page=.

[32] Court of Appeal of Rwanda: Judgment in the case of Sankara Callixte et al. vs. the Prosecution of Rwanda. Case No. RPA 00060/2021/C of April 4, 2022.

judicial officials, and investing in technological infrastructure to facilitate the collection and analysis of electronic evidence.

The issue of privacy rights and surveillance related to electronic evidence is also apparent in the same case. The interception of communications and monitoring of social media activities raise substantial privacy concerns, especially when introduced as evidence in criminal proceedings. This case has sparked discussions about the legality and ethical considerations surrounding the collection of electronic evidence through surveillance methods.

4. Lessons and best practices for Rwanda from some EU countries in the utilization of electronic evidence in cyber-crimes

Rwanda faces the challenge of effectively utilizing electronic evidence to address cyber crime cases, whether during investigation, prosecution, or adjudication. Drawing insights and lessons from the experiences of European Union (EU) countries can provide valuable guidance for Rwanda to enhance its strategies in handling electronic evidence. Some EU countries are advanced in legal frameworks, technological infrastructure, and expertise in addressing cybercrimes, justifying the relevance of this selection.

Indeed, numerous countries in the EU have established sophisticated systems and methodologies for employing electronic evidence in cybercrime cases.[33] By studying the experiences of specific EU countries such as Germany, the Netherlands, Sweden, Estonia, etc., Rwanda can acquire valuable insights in this crucial domain. This article will focus on four specific countries: Germany, the Netherlands, Sweden, and Estonia. This focus is chosen due to the practical limitations of analyzing all EU countries comprehensively.

4.1. Germany

Germany has made substantial progress in utilizing electronic evidence to counter cyber crimes. The nation has set up dedicated cyber-crime units within law enforcement agencies equipped with advanced technological capabilities for

[33] Adam Juszczak – Elisa Sason: The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice. An Introduction to the New EU Package on E-evidence. *Eucrim*, 2/2023, 182–200. https://doi.org/10.30709/eucrim-2023-014.

managing electronic evidence.[34] Rwanda can benefit from Germany's focus on specialized training for law enforcement personnel, ensuring their effectiveness in collecting, analyzing, and presenting electronic evidence in court.

4.2. The Netherlands

The Netherlands is actively working to address challenges related to electronic evidence in cyber-crime investigations by promoting partnerships between law enforcement, technology experts, and academia.[35] Rwanda can benefit from adopting a similar strategy, fostering collaboration and knowledge exchange among multiple stakeholders to handle electronic evidence more effectively.

4.3. Sweden

Swede has placed a significant emphasis on investing in research and development to advance cuttin-edge technologies for digital forensics and the analysis of electronic evidence.[36] Rwanda can benefit from studying Sweden's initiatives, which highlight the importance of staying updated on emerging trends and advancements in digital forensics tools and techniques to address cyber-crimes effectively.

4.4. Estonia

Estonia serves as a model for the effective utilization of electronic evidence in combating cybercrime, showcasing a robust legal and technological framework. As a highly digitalized nation, Estonia has implemented advanced e-governance systems that integrate secure digital signatures, blockchain technology, and interoperable databases, ensuring the authenticity, integrity, and admissibility

[34] Nikolaus Forgó et al.: The Collection of Electronic Evidence in Germany. A Spotlight on Recent Legal Developments and Court Rulings. In: Marcelo Corrales – Mark Fenwick – Nikolaus Forgó (eds.): *New Technology, Big Data, and the Law*. Singapore, Springer, 2017. 251-279.

[35] Sander Veenstra et al.: Fighting Crime in a Digitized Society: The Criminal Justice System and Public-Private Partnerships in the Netherlands. In: Wouter Stol – Jurjen Jansen (eds.): *Cybercrime and the Police.* , Hague, Eleven International Publishers, 2013. 75-87.

[36] Maria Stoyanova et al.: A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, 2/2020, 1191-1221.

of electronic evidence.[37] Its Cybersecurity Strategy emphasizes public-private partnerships, enabling seamless cooperation between law enforcement, technology companies, and judicial authorities in handling digital evidence. Estonia's adoption of the European Union's directives on electronic evidence, coupled with specialized cybercrime units and training for legal professionals, strengthens its capacity to address complex cybercrimes.[38] These practices offer valuable lessons for Rwanda, particularly in leveraging technology to enhance the collection, preservation, and presentation of electronic evidence within a clear legal framework.[39] This approach allows for a more efficient and knowledgeable handling of cyber-crime cases within the European Union.

5. Potential legal solutions for the efficient use of electronic evidence in cyber-crime within the Rwandan legal framework

The effective utilization of electronic evidence plays a pivotal role in the successful prosecution and adjudication of cyber-crimes. To enhance this aspect, the Rwandan legal framework can explore various potential legal solutions to ensure the efficient use of electronic evidence in the fight against cyber-crime.

5.1. Strengthening legal provisions for electronic evidence

One potential legal solution involves reinforcing the legal provisions on electronic evidence within the Rwandan legal framework. This may entail the creation of specific legislation addressing the admissibility, authenticity, and reliability of electronic evidence during court proceedings. By explicitly outlining the criteria for admitting electronic evidence and establishing protocols for its collection, preservation, and presentation in court, the legal framework can offer clear guidance and direction for law enforcement agencies and judicial authorities.

[37] Republic of Estonia, Information System Authority. *Cybersecurity in Estonia 2020.* Accessed on December 28, 2024. https://ria.ee/en/news/cyber-security-estonia-2020.

[38] Cyber Security in Estonia 2020 explains the landscape, the responsibilities and activities of different public sector organizations in Estonia who all contribute to keep Estonians safe online. From setting up a cyber security standard to combating cyber crime to training military cyber defence operators, every agency has a vital role to play.

[39] Heli Tiirmaa-Klaar et al.: Botnets, cybercrime and national security. In: Heli Tiirmaa-Klaar et al. (eds.): *Botnets*. Springer, 2013.1-40.

5.2. International cooperation and mutual legal assistance

International cooperation and mutual legal assistance can help Rwanda overcome challenges related to the efficient use of electronic evidence in cyber-crime within its legal framework. This can be done by exploring ways of international cooperation and mutual legal assistance in handling electronic evidence related to cyber-crimes. Establishing formal mechanisms for cooperation with other countries in areas such as data sharing, cross-border investigations and extradition of cyber criminals can significantly enhance Rwanda's ability to access electronic evidence stored outside its jurisdiction.[40] This can be achieved through bilateral or multilateral agreements that facilitate the exchange of electronic evidence while respecting data privacy and human rights considerations. Some benefits of international cooperation include:

5.2.1. Sharing of best practices

In Rwanda, the exchange of effective strategies to combat cyber-crimes is a critical element in tackling the increasing threats in the digital sphere. The nation has actively participated in regional and global efforts to strengthen cybersecurity measures and responses to cyber-crime. An example of this involvement is Rwanda hosting the 9th Africa Working Group Meeting on Cyber-Crime for Head of Units (AF-WGM) organized by INTERPOL. This event signifies Rwanda's commitment to collaborating with international partners and implementing best practices in addressing cyber threats. Collaboration with other countries allows Rwanda to learn from their experiences and implement best practices in handling cyber-crime cases.

5.2.2. Access to technical expertise

Partnering with countries possessing strong technical expertise presents a valuable opportunity for Rwanda to enhance its capacity to gather electronic evidence from digital devices and online platforms. Through knowledge transfer, capacity-building initiatives, access to advanced tools, international collaboration, enhanced credibility, legal framework alignment, resource allocation planning, and sustainability efforts, Rwanda can strengthen its capabilities in digital investigations and cyber-security.

[40] Roger Généreux Ishimwe: *Critical analysis on the impact of cybercrimes on intellectual property rights under Rwanda legal framework*. Kigali Independent University ULK, 2024. Available at: http://drepository.ulk.ac.rw:8080/xmlui/bitstream/handle/123456789/362/CRITICAL%20ANALYSIS%20ON%20THE%20IMPACT%20OF%20CYBERCRIMES.pdf?sequence=1&isAllowed=y.

5.2.3. Strengthening legal frameworks

Many types of crime, including terrorism, trafficking in human beings, child sexual abuse, and drug trafficking, have moved online or are facilitated online. As a consequence, most criminal investigations have a digital component.[41] Collaboration with other countries can help Rwanda update its legal framework to address cyber-crime better and improve the acquisition and admissibility of electronic evidence.

5.2.4. Enhancing cross-border cooperation

Cyber-criminals often operate from jurisdictions where they believe they can evade detection or prosecution. In such situations, international cooperation becomes essential to ensure that justice is served effectively. International cooperation enhances the fight against cyber-crime by sharing information and evidence. This collaboration allows law enforcement agencies to pool their resources and expertise to investigate and prosecute complex cyber-crime cases that may involve multiple jurisdictions. For instance, Rwanda may need assistance from foreign experts to analyze digital evidence or trace the origin of an attack. By working together, law enforcement agencies can increase their chances of identifying and apprehending cyber-criminals.

Moreover, international treaties and agreements provide a legal framework for cross-border cooperation in cybercrime investigations. For example, the Council of Europe's Convention on Cyber-Crime, known as the Budapest Convention, sets out specific provisions for mutual legal assistance and extradition in cyber-crime cases. The United Nations Convention on Transnational Organized Crime also includes provisions for addressing cyber-crime. These treaties help ensure that countries follow established procedures when requesting assistance from each other in cyber-crime investigations[42].

International cooperation can facilitate the exchange of information and evidence between countries, making it easier for Rwandan authorities to work with their foreign counterparts in investigating and prosecuting cyber- crime cases.

[41] Anita Lavorgna: *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes. Doctoral Thesis*. University of Trento, 2014. https://iris.unitn.it/handle/11572/368968.

[42] United Nations Office on Drugs and Crime (UNODC) (2020). *Global Cybercrime Report 2020.* https://www.unodc.org/global/publications/2020/e38547_global_cybercrime_report_2020.pdf.

5.3. Promoting public awareness and collaboration

Cyber-crimes' complex and evolving nature necessitates a collaborative strategy that engages various stakeholders. This strategy leverages diverse entities' expertise, resources, and authority, enabling them to cooperate in sharing information, advancing technology, and developing impactful policies. This multi-stakeholder approach strives to address cyber-crimes and comprehensively protect citizens' digital rights through united endeavors.

Enhancing public awareness about the importance of electronic evidence in combating cyber-crimes is crucial. Collaborative efforts involving government agencies, private sector entities, academic institutions and civil society organizations can raise awareness about cyber security risks, digital hygiene practices, and reporting mechanisms for cyber incidents. By fostering a culture of collaboration and information sharing, Rwanda can create a supportive environment for effectively leveraging electronic evidence to address cyber threats. This collaboration can lead to several benefits in addressing the challenges of electronic evidence in cyber crimes within the Rwandan legal system:

5.3.1. Improved capacity to investigate and prosecute cyber-crimes

Collaboration enables the sharing of resources, expertise, and technology, which can significantly enhance the capacity of law enforcement agencies to investigate and prosecute-cyber-crimes. By sharing resources, exchanging expertise, and integrating technology, these agencies can enhance their collective ability to combat the growing menace of cyber threats. Through coordinated efforts and mutual support, law enforcement can stay ahead of cyber-criminals and ensure a safer digital environment for individuals and organizations worldwide[43].

5.3.2. Enhanced cyber-security

Enhanced cyber-security through collaboration is crucial in combating the ever-evolving landscape of cyber threats. By leveraging collective expertise, resources, and innovation capabilities through collaborative initiatives, stakeholders can strengthen their defenses and better protect individuals and critical infrastructure from malicious cyber activities[44]. Collaboration can lead to the development of advanced cyber-security solutions that protect citizens and critical infrastructure from cyber threats.

[43] Federal Bureau of Investigation: Cyber Security Incident Management: Collaborating with Law Enforcement 2024, https://moldstud.com/articles/p-cyber-security-incident-management-collaborating-with-law-enforcement/pdf.

[44] Ibid. 33.

5.3.3. Strengthened legal framework. Collaboration can contribute to developing a robust legal framework that addresses the challenges of electronic evidence in cyber-crimes, including the admissibility of digital evidence in court. Collaboration among various stakeholders is indispensable for developing a robust legal framework that effectively addresses the challenges associated with electronic evidence in cybercrimes. By leveraging collective expertise, fostering cross-disciplinary partnerships, ensuring international cooperation, and promoting innovation, stakeholders can enhance legal practices related to digital evidence admissibility and strengthen the overall response to cyber threats[45].

5.3.4. Increased public awareness and trust

Collaboration among various stakeholders, including government agencies, law enforcement, cyber-security experts and the public, is crucial in raising awareness about cyber crimes and the importance of reporting such incidents. By working together, these entities can educate the public about the risks associated with cyber threats, the methods used by cyber-criminals and the potential impact of these crimes on individuals, businesses, and society as a whole[46]. Collaboration can also raise public awareness about cyber crimes and the importance of reporting such incidents, leading to increased confidence in the legal system and its ability to address these challenges.

5.4. Establishing digital forensics units

Establishing specialized digital forensics units within law enforcement agencies or judicial bodies is an essential step in establishing digital forensics units. These units can be equipped with the necessary expertise and technology to effectively collect, analyze, and present electronic evidence in cyber-crime investigations and court proceedings[47]. By investing in training programs and technological resources for digital forensics, Rwanda can enhance its capacity to handle electronic evidence in a manner that meets international forensic investigation standards.

[45] Council of Europe 2020, 31.

[46] Joanna Curtis – Gavin Oxburgh: Understanding cyber-crime in 'real world' policing and law enforcement. *The Police Journal*, 4/2023, 573–592. https://doi.org/10.1177/0032258X221107584.

[47] United Nations Office on Drugs and Crime: Establishing specialized digital forensic units within law enforcement agencies or judicial bodies 2019, https://www.unodc.org/documents/organized-crime/Publications/UNODC_Digital_Forensics_Handbook.pdf.

5.5. Capacity Building and Training

Capacity-building and training programs are essential for legal professionals, law enforcement officers, and judicial personnel handling electronic evidence. Comprehensive training on digital forensics, cyber-crime investigation techniques, and the legal aspects of electronic evidence can improve the competence of relevant stakeholders in dealing with complex cyber-crime cases. Additionally, continuous professional development initiatives can keep them abreast of evolving technologies and best practices in managing electronic evidence[48].

5.6. Creation of Specialized Cybercrime Courts

The criminal landscape has evolved with the advancement of technology, giving rise to a surge in cyber crimes. These crimes often involve electronic evidence and present unique investigation, prosecution, and adjudication challenges. While Rwanda has specialized courts for specific matters such as commerce, family and minors, economic crimes, and administrative labor cases, there must be a more significant gap in addressing cyber crimes.

Introducing specialized cybercrime courts is a potential legal solution to tackle the hurdles of using electronic evidence in Rwandan cyber-crime cases. Drawing inspiration from the best practices, such as those implemented in Estonia, these dedicated courts could feature judges with specialized knowledge in handling cyber-related cases. This approach ensures that electronic evidence is thoroughly assessed and effectively incorporated into the legal system.

6. Conclusion

This paper emphasizes the importance of effectively utilizing electronic evidence in addressing cybercrime within Rwanda's legal framework. Electronic evidence, stored on computers, smartphones, and other digital devices, plays a pivotal role in uncovering cyber-crimes' nature, scope, and perpetrators. Leveraging this evidence is essential for building strong cases and ensuring offenders are brought to justice.

A comprehensive, multi-faceted approach is necessary to address the challenges of integrating electronic evidence into Rwanda's legal processes. This includes

[48] Ibid. 14.

enacting specific legislation to guide the collection, storage, and presentation of electronic evidence in a manner that aligns with international best practices. Additionally, establishing digital forensic standards and providing specialized training for law enforcement, judges, and legal practitioners are crucial for effectively enhancing their capacity to handle electronic evidence in cybercrime cases. One of the key measures proposed is the creation of specialized cybercrime courts equipped with judges, prosecutors, and investigators trained in digital forensics and cybercrime investigations. These dedicated courts would have the expertise and authority to adjudicate cases involving hacking, online fraud, data breaches, and other cyber offenses, ensuring that legal proceedings meet both domestic and international standards. This approach would expedite the adjudication of cybercrime cases and foster the development of a deep pool of expertise in handling electronic evidence within the judicial system.

Moreover, the establishment of dedicated cybercrime units within law enforcement agencies, supported by advanced technological tools, will significantly enhance Rwanda's capacity to detect, investigate, and prosecute cybercriminals. Through cooperation with international partners, Rwanda can facilitate cross-border investigations and share vital intelligence on emerging cyber threats, further strengthening its ability to combat global cybercrime.

The paper highlights the need for a holistic strategy combining legal reforms, technical advancements, specialized training, and international collaboration to enhance Rwanda's capacity to combat cybercrime by effectively utilizing electronic evidence. By adopting these critical measures, Rwanda will improve its response to cyber threats and contribute to fostering a more secure and resilient digital environment, both nationally and globally. These reforms will ensure that Rwanda remains at the forefront of efforts to combat cybercrime in the digital age.

Bibliography

Scott H. Belshaw: Next Generation of Evidence Collecting. The Need for Digital Forensics in Criminal Justice Education. *Journal of Cybersecurity Education, Research and Practice*, 1/2019. https://files.eric.ed.gov/fulltext/EJ1341743.pdf.

Bernard Walumoli: *A Critical Analysis of the Challenges Facing Countercybercrime in 21st Century Africa: a Focused Comparison of Kenya and Rwanda. Diss.* University of Nairobi, 2021.

Nikolaus Forgó et al.: The Collection of Electronic Evidence in Germany. A Spotlight on Recent Legal Developments and Court Rulings. In: Marcelo Corrales – Mark Fenwick – Nikolaus Forgó (eds.): *New Technology, Big Data, and the Law*. Singapore, Springer, 2017. 251-279.

Jonah Force Hill – Matthew Noyes: *Rethinking Data, Geography, and Jurisdiction. Towards A Common Framework for Harmonizing Global Data Flow Controls*. New America and Cybersecurity Initiative, 2018.

Ki Hong Steve Chon: *Cybercrime precursors. Towards a model of offender resources. Doctor of Philosophy dissertation*. Australian National University, 2016.

Roger Généreux Ishimwe: *Critical analysis on the impact of cybercrimes on intellectual property rights under Rwanda legal framework*. Kigali Independent University ULK, 2024. Available at: http://drepository.ulk.ac.rw:8080/xmlui/bitstream/handle/123456789/362/CRITICAL%20ANALYSIS%20ON%20THE%20IMPACT%20OF%20CYBERCRIMES.pdf?sequence=1&isAllowed=y.

Adam Juszczak – Elisa Sason: The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice. An Introduction to the New EU Package on E-evidence. *Eucrim*, 2/2023, 182–200. https://doi.org/10.30709/eucrim-2023-014.

Peter A. Joy: Prosecution Clinics. Dealing with Professional Role. *Mississippi Law Journal*, 4/2005, 955–981. https://heinonline.org/HOL/LandingPage?handle=hein.journals/mislj74&div=40&id=&page=.

Jacques Kabano – Jean Habarurema: Procedural Aspects of Cyber Crimes Investigations in Rwanda. A Comparative Study. *Makerere Law Journal*, 5/2023, 240–266.

Bradley Lawrence Schatz: *Digital evidence, representation, and assurance. Diss*. Queensland University of Technology, 2007.

Anita Lavorgna: *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes. Doctoral Thesis*. University of Trento, 2014. https://iris.unitn.it/handle/11572/368968.

Ronald Serwanga: *Legal mechanisms for enforcing electronic transactions in Rwanda. Diss.* University of Rwanda, 2019.

Maria Stoyanova et al.: A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, 2/2020, 1191-1221.

Allan Thompson (ed.): *The Media and the Rwanda Genocide*. London, Pluto Press, 2007. https://doi.org/10.2307/j.ctt18fs550.

Heli Tiirmaa-Klaar et al.: Botnets, cybercrime and national security. In: Heli Tiirmaa-Klaar et al. (eds.): *Botnets*. Springer, 2013.1-40.

PROSECUTION AND CONTROL OF CYBERCRIME IN RWANDA. LEGAL STRATEGIES AND ENFORCEMENT PRACTICES

Francois Regis Nshimiyimana[1]

ABSZTRAKT ■ Ez a tanulmány Ruanda jogi stratégiáit és bűnüldözési mechanizmusait vizsgálja a kibertámadások növekvő kihívásának kezelésére. Ruanda jogi keretrendszerét és bűnüldözési képességeit próbára teszik a fejlődő digitális fenyegetések, amelyek rámutatnak az eredményes büntetőeljárás és bűnmegelőzés hiányosságaira. A tanulmány kísérletet tesz a hatályos jogszabályok elemzésére, a bűnüldöző hatóságok által tapasztalt gyakorlati kihívások értékelésére, valamint a fejlesztést elősegítő javaslatok megfogalmazására. Összehasonlító jogi elemzések, esettanulmányok, illetve jogi szakemberekkel és bűnüldöző szervekkel folytatott interjúk révén jelen tanulmány célja, hogy értékelje a jelenlegi gyakorlatok hatékonyságát, és reformokat javasoljon Ruanda kiberbűnözés elleni küzdelemre irányuló erőfeszítéseinek javítására.

ABSTRACT ■ This paper investigates Rwanda's legal strategies and enforcement mechanisms to address the growing challenge of cybercrime. Rwanda's legal framework and law enforcement capabilities are tested as digital threats evolve, revealing effective prosecution and crime prevention gaps. The study seeks to analyze the existing legal provisions, assess enforcement agencies' practical challenges, and propose improvement measures. Through a comparative legal analysis, case studies, and interviews with legal professionals and law enforcement, this paper aims to evaluate the effectiveness of current practices and suggest reforms to enhance Rwanda's cybercrime control efforts.

Keywords: cybercrime, enforcement practices, cyber-security

1. Introduction

The emergence of digital technology in Rwanda has led to a notable rise in cybercrime rates, creating new obstacles for the nation's legal and enforcement frameworks[2]. Cybercrime, which ranges from sophisticated computer attacks to

[1] PhD student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

[2] William Maluleke: Exploring Cybercrime. An Emerging Phenomenon and Associated Challenges in Africa. *International Journal of Social Science Research and Review*, 6/2023, 223–243.

online fraud[3], is a hazard to persons and institutions, underscoring the necessity for efficient legal and regulatory responses.

1.1. Methodology

This study adopts a qualitative research approach, analyzing Rwanda's existing legal framework, relevant laws, and policies on cybercrime and electronic evidence. The research involves a review of academic literature, legal texts, and case law to identify gaps and challenges in the current system. A comparative analysis of international best practices will also be conducted to propose feasible solutions adapted to Rwanda's legal and technological context. The study aims to comprehensively understand the obstacles in utilizing electronic evidence in Rwanda's cybercrime cases and suggest practical recommendations for strengthening the legal framework to address these challenges effectively.

1.2. Background of the study

Digital technology has brought globalization to all walks of life and presents opportunities for communication and criminal activities. Cybercrime, or computer-oriented crime, is a severe threat threatening a person or a nation's security and financial health[4]. Cybercrimes involve computers and networks, and their issues include hacking, copyright infringement, mass surveillance, sex extortion, child pornography, and child grooming. Privacy problems arise when confidential information is intercepted or disclosed. Cybercrimes cross international borders and involve governmental and non-state actors, including espionage, financial theft, and other cross-border crimes. Understanding cybercrime phenomena, including challenges in prosecution and punishment, aims to assist countries in understanding the legal aspects of cyber security and

[3] Hamid Jahankhani – Ameer Al-Nemrat – Amin Hosseinian-Far: Cybercrime Classification and Characteristics. In: Babak Akhgar – Andrew Staniforth – Francesca Bosco (eds.): *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Waltham, Syngress, 2014. 149–164.

[4] Fidelis Chukwunenye Obodoeze: "Cyber Crimes. Effects of Information Technology and Globalization on World Economy." Paper presented at the UNESCO World Philosophy Day Celebration Workshop, Nnamdi Azikiwe University, Awka, Nigeria, November 21-23, 2011. https://www.researchgate.net/publication/340333512_CYBER_CRIMES_EFFECTS_OF_INFORMATION_TECHNOLOGY_AND_GLOBALIZATION_ON_WORLD_ECONOMY.

harmonizing legal frameworks[5]. Challenges faced by prosecution and punishment actors include data loss, location loss, lack of legal framework, public and private partnerships, international cooperation, and evolving threat landscape[6].

1.3. General overview of cybercrime

Cybercrime is a global issue affecting electronic activities and involves crimes committed online using computers as tools or victims[7]. Classifying crimes into distinct groups is challenging due to the constantly evolving nature of cybercrime. The main target of cybercrimes depends on the computer and the person behind it. The unity of international, regional, and local governments is crucial in fighting against cybercrime and preventing danger caused by the Internet, networks, and computer systems. Cybercrime is a social label, not an established term within criminal law, and includes traditional and coming crimes conducted through computers and the Internet[8].

2. Forms of cybercrime activities

The prevalence of cybercrime activities in contemporary society has escalated, posing significant threats to governments, individuals, and businesses globally. With the rapid advancement of communication technologies, the number of cybercrime victims has surged, leading to various forms of harm such as harassment, financial losses, and considerable economic costs.9 While some of the impacts of cybercrime can be quantified in monetary terms, the broader consequences extend far beyond financial figures.[10]

5 Anja P. Jakobi: Non-State Actors All Around. The Governance of Cybercrime. In: Anja P. Jakobi – Klaus Dieter Wolf: *The Transnational Governance of Violence and Crime. Non-State Actors in Security*. London, Palgrave Macmillan, 2013. 129–148.

6 Cameron Scott Doran Brown: Investigating and Prosecuting Cyber Crime. Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, 1/2015, 55–119. 55. Available at: https://cybercrimejournal.com/pdf/Brown2015vol9issue1.pdf.

7 Sumanjit Das – Tapaswini Nayak: Impact of Cyber Crime. Issues and Challenges. *International Journal of Engineering Sciences & Emerging Technologies*, 2/2013, 142–153. Available at: https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf.

8 Ibid.

9 Richard Anderson et al.: "Measuring the Changing Cost of Cybercrime". Paper presented at The 18th Annual Workshop on the Economics of Information Security (WEIS 2019), Boston, 2019. https://weis2019.econinfosec.org/program/agenda/.

10 Ibid.

– Intellectual property (IP) theft is a major form of cybercrime involving the unlawful appropriation of commercial trademarks, patents, and copyrighted works such as music, movies, and books.[11] Cybercriminals use advanced technological means to steal vast amounts of copyrighted material, severely impacting the businesses or individuals victimized by such acts. Online piracy is a widespread form of IP theft, targeting consumers seeking discounted yet genuine products.[12]

– Hacking refers to unauthorized access to computer systems and networks, typically by individuals possessing specialized knowledge in coding or programming.[13] These cybercriminals exploit vulnerabilities to steal sensitive data or engage in illicit activities on behalf of others. Hackers often manipulate system controls or install malware to gain entry into target networks and commit further cybercrimes.[14]

– Child grooming is another harmful activity that exploits the internet to facilitate illegal businesses, including child prostitution and the production of child pornography.[15] Grooming typically involves building an emotional connection with a minor to reduce their inhibitions and manipulate them into abusive situations.[16] This form of exploitation is often perpetrated by adults with a sexual attraction to children.

– Identity theft and the stealing of sensitive data occur when cybercriminals successfully acquire personally identifiable information (PII). This information is often used for financial gain or to inflict damage on the victim.[17] Identity theft can involve activities such as unauthorized credit card transactions, online purchases, or renting property, all facilitated through illicit access to an individual's personal data.

– Cyber-stalking is a growing concern, wherein offenders use digital communication methods such as email to harass or threaten their victims. Unlike offline stalking, which involves physical proximity, cyber-stalking can be especially insidious, as it allows the stalker to remain anonymous and unseen while

11 David S. Wall – Majid Yar: Intellectual Property Crime and the Internet. Cyber-Piracy and 'Stealing' Information Intangibles. In: Yvonne Jewkes – Majid Yar (eds.): *Handbook of Internet Crime*. 2nd ed., Oxford, Routledge, 2011. 230-255.

12 Ibid.

13 Robert J. Sciglimpaglia, Jr.: Computer Hacking. A Global Offense. *Pace Yearbook of International Law*,1/1991, 199–266. 199. https://digitalcommons.pace.edu/pilr/vol3/iss1/.

14 Ibid.

15 Kim-Kwang Raymond Choo: *Online Child Grooming. A Literature Review on the Misuse of Social Networking Sites for Grooming Children for Sexual Offences*. Canberra, Australian Institute of Criminology, 2009. https://www.aic.gov.au/sites/default/files/2020-05/rpp103.pdf.

16 Ibid.

17 Clapper v. Amnesty International USA, 568 U.S. 398, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013).

causing significant emotional distress.[18] This form of harassment often leads to victims fearing for their safety, with stalkers engaging in repeated and threatening behaviors.[19]

– Computer and internet fraud involves using computer systems to engage in deceptive practices that mislead others into making decisions that lead to financial loss.[20] Fraudsters may alter input data, manipulate stored information, or install malicious software to facilitate crimes.[21] For example, cybercriminals may rewrite software codes and infiltrate banking systems, enabling unauthorized transactions using stolen user credentials.

– Computer malware, including viruses and worms, is a form of malicious software designed to damage or disrupt computer systems. Malware is often spread through the internet, particularly via email attachments or downloadable files , and can cause significant harm by corrupting data, deleting files, or rendering systems inoperable.[22] Cybercriminals use malware to exploit vulnerabilities in computer systems, enabling them to carry out further malicious actions or steal sensitive information.[23] The widespread nature of these cybercrimes underscores the urgent need for robust cybersecurity measures and international cooperation to combat these threats.

3. The legal framework for addressing Cybercrimes in Rwandan legislation

Rwanda has developed a robust legal framework to combat cybercrimes, demonstrating its commitment to improving cybersecurity and safeguarding its citizens in the digital era. Legislation that tackles a wide range of cyber offenses is necessary because, as technology advances, so do the tactics used by hackers. The

[18] Michael Pittaro: Cyberstalking. An Analysis of Online Harassment and Intimidation. *International Journal of Cyber Criminology*, 2/2007, 180–197.

[19] John Reid Meloy: Stalking. An Old Behavior, A New Crime. *Psychiatric Clinics of North America*, 1/1999, 85–99. https://www.sciencedirect.com/science/article/abs/pii/S0193953X05700617.

[20] Samuel W. Buell: What Is Securities Fraud. *Duke Law Journal*, 3/2011, 511–581. 511.

[21] John Aycock: *Computer Viruses and Malware.* New York, Springer Science & Business Media, 2006. 1-8.

[22] Thomas M. Chen – Jean-Marc Robert: The Evolution of Viruses and Worms. In: William W.S. Chen (ed.): *Statistical Methods in Computer Security*. Boca Raton, CRC Press, 2004. 289-310. https://www.taylorfrancis.com/chapters/edit/10.1201/9781420030884-19/evolution-viruses-worms-thomas-chen-jean-marc-robert.

[23] Ibid.

Rwandan government has realized how critical it is to enact laws and rules that discourage cybercrime and offer channels for victim assistance and prosecution.

3.1. Law nº68/2018 of 30/08/2018 determining offences and penalties in general

According to the above law, which governs general principles governing offenses and penalties, article 160 regarding the Collection of individuals' personal information in computers states that "Any person who, in bad faith, records, collects an individual's personal information or who archives or uses other ways of keeping the personal information in computers and other specialized equipment in a manner that is likely to adversely affect the individual's honor or his/her privacy, commits an offense.[24] Upon conviction, he/she is liable to imprisonment for a term of not less than six (6) months and not more than one (1) year and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than two million Rwandan francs (FRW 2,000,000)".[25] Acts referred to in Paragraph One of this article performed professionally or in the context of one's duty and legally recognized do not qualify as an offense.

3.2. Law n°24/2016 of 18/06/2016 governing information and communication technologies

This Law establishes a framework for Information and Communication Technologies (ICT) policy and regulation. Article 198, regarding access to a computer system with the intent to commit an offense, provides that "any person who causes a computer system to perform any function to secure access to any program or data held in any computer system with the intent to commit an offense is punished under the provisions of the penal code".[26] Any individual who, through any means, knowingly gains unauthorized access to a computer system to obtain, either directly or indirectly, any computer service, function, or data within the system, commits an offense. This is punishable by the provisions of the Penal Code. However, a person shall not be guilty of an offense if they

[24] Article 160 of Law n°68/2018 of 30/08/2018 determining offences and penalties in general, Officicial Gazette no special of 27/09/2018.

[25] Ibid.

[26] Article 198 of Law n°24/2016 of 18/06/2016 governing information and communication technologies, Official Gazette n°26 of 27/06/2016.

have obtained consent from the individual who sent the data and the intended recipient or is acting within the bounds of any statutory authority.[27]

In addition, any person knowingly engaging in activities that result in the unauthorized modification of data held within a computer system is committing an offense. This act is punishable under the relevant provisions of the penal code.[28] Furthermore, anyone without lawful authority or excuse who performs an act that directly or indirectly causes degradation, failure, interruption, or obstruction of a computer system's operation or denies access to or damages any program or data stored within the system is guilty of an offense. This, too, is punishable under the provisions of the Penal Code.[29]

The unlawful possession of computer systems, devices, and data constitutes a crime. A person who knowingly manufactures, sells, procures, imports, distributes, or otherwise makes available a computer system or any device while possessing data or programs intending to use them or enable others to commit an offense personally is guilty of an offense. This is punishable by the penal code.[30]

Similarly, any individual who, by means of a computer or electronic device, commits fraud or facilitates or causes forgery is committing an offense. This is punishable under the relevant provisions of the penal code.[31]

Additionally, the disclosure of passwords or access codes constitutes a criminal offense if it is made knowingly and to obtain wrongful gain or for an unlawful purpose and if it is likely to cause harm to another individual. According to the penal code's provisions, a person guilty of this offense will face punishment.[32] Finally, any individual who knowingly or willfully publishes or transmits indecent information in electronic form or causes such information to be published commits an offense, punishable under the relevant provisions of the penal code.

3.3. Law nº18/2010 of 12/05/2010 relating to electronic messages, electronic signatures, and electronic transactions

To create a thorough legal framework that encourages and governs the use of electronic communications and digital transactions in Rwanda, Law No. 18/2010 of 12/05/2010 was passed. This law deals with electronic messages,

27 Article 199, Law n°24/2016 of 18/06/2016, 24.
28 Article 200, Law n°24/2016 of 18/06/2016, 23.
29 Article 201, Law n°24/2016 of 18/06/2016, 23.
30 Article 202, Law n°24/2016 of 18/06/2016, 23.
31 Article 203, Law n°24/2016 of 18/06/2016, 23.
32 Article 204, Law n°24/2016 of 18/06/2016, 23.

electronic signatures, and electronic transactions. With the nation increasingly incorporating digital technologies into its economic and social structure, this law seeks to guarantee electronic transactions' legitimacy, security, and dependability. It creates explicit rules for digital signatures, electronic messaging, and general online business conduct, which promotes confidence and helps expand digital services and e-commerce while guarding against fraud and other online hazards.

3.3.1. Unauthorized access to computer data

Access by a person to a computer system is unauthorized where the person is not entitled to control and access the computer system; does not have consent to access by him/her of the kind in question from any person who is so entitled[33]. Any person who causes a computer system to perform a function, knowing that the access he/she intends to secure is unauthorized, shall commit an offense but shall not be liable under this provision where he/she is a person entitled to control the operation or use of the computer system and exercises such right in good faith. He/she has the express or implied consent of the person empowered to authorize him/her to have such access; he/she is acting in reliance of any statutory power arising under any enactment to obtain information or take possession of any document or other property.[34] For this section, any access not directed at any particular program or data, a program or data of any kind, or a program or data held in any specific computer system shall be immaterial.

3.3.2. Access to a computer system with the intent to commit offenses

Any person who causes a computer system to perform any function to secure access to any program or data held in any computer system, with intent to commit an offense under any law, commits an offense.[35]

3.3.3. Unauthorized access to and interception of computer service

Any person who, by any means, knowingly has unauthorized access to any computer system to obtain, directly or indirectly, any computer service or intercepts or causes to be intercepted, directly or indirectly, any function or any data within a computer system commits an offense.[36]

[33] Peter A. Winn: The guilty eye. Unauthorized access, trespass, and privacy. *The Business Lawyer*, 4/2007, 1395–1437.

[34] Article 58 of Law nº 18/2010 of 12/05/2010 relating to electronic messages, electronic signatures, and electronic transactions, *O.G n° 20 of 17/05/2010.*

[35] Ibid. Article 59.

[36] Ibid.

Institutional framework

The institutional framework for addressing cybercrime in Rwanda is designed to combat and prevent digital offenses through a coordinated approach involving various government agencies and regulatory bodies. Rwanda's National Cyber Security Authority (NCSA) plays a central role in safeguarding the country's digital infrastructure and implementing robust security measures. Established under Law No.26/2017 of May 31, 2017, the NCSA is mandated to protect national interests and combat the growing threat of cybercrime.[37] Its responsibilities include developing and executing comprehensive cybersecurity plans, conducting response exercises, and promoting industry best practices. The institutional framework of the NCSA also encompasses public awareness campaigns, threat intelligence, policy formulation, and incident response, all of which significantly enhance Rwanda's cyber defenses and security posture.[38]

According to Article 4 of Law No.26/2017 of May 31, 2017, the NCSA's mission focuses on building skills and capacities in cybersecurity to protect national integrity and security while supporting economic and social development. To achieve these goals, the NCSA advises the President of the Republic and other public and private institutions on strategies to protect Rwanda's interests in cyberspace. It conducts cyber intelligence to identify threats to national security, shares intelligence with appropriate organs, establishes guidelines based on national and international ICT security principles, and coordinates the implementation of a national ICT security policy and strategy.[39]

The NCSA is also responsible for developing plans to secure electronic operations, monitoring national ICT security programs, preventing cyber-attacks, and protecting critical ICT infrastructure. Additionally, the authority fosters national cybersecurity education, promotes research and industry development in the ICT sector, raises public awareness about cybersecurity, and collaborates with regional and international bodies to enhance ICT security. It supports national defense and security organs in cyberspace and performs other duties the President assigns.[40]

As stipulated by Law No.26/2017, the powers granted to the NCSA include setting guidelines for cyberspace protection and ICT security, conducting critical

37 Article 4 of law no 26/2017 of 31/05/2017 establishing the national cyber security authority and determining its mission, organization, and functioning, *O.G nº 27 of 03 July 2017.*

38 Ibid.

39 Roger Généreux Ishimwe: *Critical analysis on the impact of cybercrimes on intellectual property rights under Rwanda legal framework*. Kigali Independent University ULK, 2024. http://drepository.ulk.ac.rw:8080/xmlui/bitstream/handle/123456789/362/CRITICAL%20ANALYSIS%20ON%20THE%20IMPACT%20OF%20CYBERCRIMES.pdf?sequence=1&isAllowed=y.

40 Article 9 of law nº 26/2017 of 31/05/2017, 37.

infrastructure audits, investigating cyber threats, and collaborating with other organizations to combat cybercrime. Despite these efforts, Rwanda continues to face challenges in addressing cybercrime, including limited cooperation, inadequate electronic evidence gathering, and logistical hurdles that impede the immediate prosecution and punishment of cybercrimes.[41]

Complementing the NCSA's efforts, the Rwanda National Police (RNP) is pivotal in combating cybercrime. The RNP's strategic plan includes infrastructure development, enhancing equipment capabilities, improving communication systems, fostering police discipline, and developing anti-corruption strategies. With the increasing use of the internet and digital technologies, the RNP has focused on implementing systems to prevent and fight against cybercrimes in collaboration with various stakeholders.[42] Criminals increasingly exploit cyberspace to access personal information, steal intellectual property, and compromise sensitive government-held data for financial, political, or other malicious purposes, necessitating a proactive response by law enforcement.[43]

The Rwanda Investigation Bureau (RIB) is another critical institution in the fight against cybercrime. Established by Law No.12/2017 of April 7, 2017, the RIB operates under the Ministry of Justice and is tasked with investigating various crimes, including cybercrime. Its responsibilities include receiving complaints on criminal behavior, gathering and assembling criminal evidence for prosecution, and ensuring the prompt and efficient disposal of cases.[44] The RIB also provides forensic services, collects and disseminates information on criminals, and develops and implements strategies to enhance cybersecurity. These roles are vital in improving Rwanda's public order, safety, and crime prevention.

The obstacles hindering Rwanda's efforts to prosecute and suppress cybercrime.

While Rwanda has advanced significantly in technology and digital transformation, the country still has a long way to go before it can prosecute and suppress cybercrime. The emergence of cyber attacks presents a significant risk to the nation's economic growth and national security as it embraces digitalization.

41 John Gacinya: *Criminal Justice System as an Instrument of Internal Security. A Case Study of Rwanda. Master's thesis*. Institute of Diplomacy and International Studies (IDIS), University of Nairobi, 2013. 75-159. https://erepository.uonbi.ac.ke/bitstream/handle/11295/166148/Criminal%20Justice%20System%20as%20an%20Instrument%20of%20Internal%20Security%20a%20Case%20Study%20of%20Rwanda.pdf?sequence=1.

42 RNP, *Strategic plan 2013-2018*, Kigali Rwanda, 1-47, Available at: https://police.gov.rw/uploads/tx_download/RNP_A5_Booklet_FINAL_2015.pdf.

43 Ibid.

44 Law n°12/2017 of April 7, 2017 establishing the Rwanda Investigation Bureau and determining, its mission, powers, organization and functioning, Official gazette no Special of 20/04/2017.

It is essential to comprehend the barriers preventing Rwanda from progressing in this area to create tactics that effectively tackle cybercrime.

4. Challenges relating to the identification of cybercriminals

This paper believes that the anonymity of cybercriminals' identities continues to be one of the most significant barriers to international attempts to curb the spiraling incidence of cybercrimes. The anonymity of cybercriminals' identities remains a substantial barrier to international efforts to combat cybercrimes.[45] The global information system's freedom allows cybercriminals to hide their identities using various telecommunications gadgets, making it impossible to trace their online IP addresses. This makes it difficult to enforce laws, as they are not meant to work in a vacuum. Cybercrime laws were primarily enacted to apprehend and prosecute cybercriminals, making investigations and punishments difficult due to the lack of physical presence.

4.1. The challenges related to jurisdiction

Jurisdiction is a crucial issue in enforcing cybercrime laws, as it affects the power of a court to entertain an action, petition, or proceeding[46]. A court needs jurisdiction to try a case, as a defect in competence can render proceedings null and void. Jurisdiction is used in intra-territorial and extra-territorial situations, with extra-territorial jurisdiction being crucial when a court's judgment is sought to be enforced outside the forum. A jurisdictional challenge to enforcing cybercrime laws reduces the hurdle of anonymity, as a court cannot effectively try a cybercriminal if they are located in another country[47]. Extradition is a solution, but it faces challenges, including double criminality requirements and the absence of extradition treaties or mutual legal assistance treaties between the requesting and custody states.

[45] Zunaira Sattar et al.: "Challenges of Cybercrimes to Implementation of Legal Framework." Paper presented at the International Conference on Emerging Technologies, November 1, 2018. https://www.semanticscholar.org/paper/Challenges-of-Cybercrimes-to-Implementation-of-Sattar-.

[46] Emmanuel Ajayi: Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, 1/2016, 1–12. https://www.researchgate.net/publication/307528405_Challenges_to_enforcement_of_cybercrimes_laws_and_policy.

[47] Idem.

4.2. The barriers relating to the processes of extradition of a suspect

Extradition is returning somebody accused of a crime to a different legal authority for trial or punishment[48]. Extradition has also been defined as the surrender by one state to another of a person accused of committing an offense in the latter[49]. A casual glance at the definition of extradition as above would ordinarily raise the hope that if a person is alleged to have committed a cybercrime in one jurisdiction and escapes to another country, all that needs to be done by the country where the cybercriminal is domiciled is expeditiously return the said criminal to the requesting country, to face trial, however, in practice, this is not so because of the principle of state independence and sovereignty earlier stated before now.[50] Under international law, no instrument obligates sovereign nations to return cybercriminals for trial automatically. In effect, countries where Cybercriminals are situated, for different reasons, more often than not refuse to extradite them, and this development presents an insurmountable challenge to the enforcement of cybercrime laws across the globe.

To address the lacuna created as a result of the lack of international law not making it mandatory to deport criminals, extradition treaties fill the void; thus, if there is a treaty between two states, criminals may be deported, and even at that, there are many exceptions to extradition processes. One of the biggest hurdles to the extradition of criminals to requesting states is the "unruly legal horse" called jurisdiction; countries often invoke jurisdiction to deny extradition[51], especially if the requested state has jurisdiction to try criminals who are nationals of the requested state; as such, the requesting state has no choice but to abide by that decision not to commence extradition.

[48] Craig R. Roecks: Extradition, Human Rights, and the Death Penalty. When Nations Must Refuse to Extradite a Person Charged with a Capital Crime. *California Western International Law Journal*, 1/1994, 189. https://heinonline.org/HOL/LandingPage?handle=hein.journals/calwi25&div=10&id=&page=.

[49] Ibid.

[50] M. Cherif Bassiouni: *The Sources and Content of International Criminal Law. A Theoretical Framework*. Leiden, Martinus Nijhoff Publishers, 1999. 353-356.

[51] Emmanuel O. C. Obidimma – Richard Onyekachi Ishiguzo: Cybercrime Investigation and Prosecution in Nigeria. The Critical Challenges. *African Journal Of Criminal Law And Jurisprudence*, 8/2023, 30–36. 30.

4.3. The challenge regarding the nature of evidence

The enforcement of cybercrime laws is hindered by the nature of the evidence available in prosecution custody and its admissibility in cybercriminals' trials[52]. Evidence can take various forms, including testimony, documentary, and tangible evidence. In criminal prosecution, it is crucial to prove the case beyond a reasonable doubt before a conviction can be obtained. However, the evidence available in cybercrime prosecution is often tenuous and needs more evidential value. Physical evidence is rare, and investigators rely on footprints on computers and internet traces, which have little evidential value and are costly to gather.

4.4. Lack of effective reporting and lack of data

Many countries have laws and policies against cybercrime, but enforcing them is challenging due to inadequate reporting and lack of cooperation between victims, stakeholders, and police. Reasons for reluctance include costs, reputation damage, lengthy investigations, and difficulty in diligent investigation. The lack of cooperation and the damage caused by cybercrimes can hinder global attention and appreciation of the menace. Addressing these issues is crucial for a more practical approach to cybercrime.

4.5. Cost, time, and efforts incurred in investigation and prosecution

The cost of using a scientific approach to solving crimes is significantly higher than traditional evidence gathering in terrestrial crimes, mainly due to the forensic evidence required for prosecuting cybercrimes.[53] This approach also demands high-tech equipment, specialized materials, and expertise to conduct investigations. In the context of business and social interactions, the rise of technology has had two main effects. On the one hand, it has brought numerous advantages, such as faster and more accurate information and communication, making the world feel like a global village. On the other hand, it has led to the rise

[52] Susan W. Brenner – Joseph J. Schwerha: Transnational Evidence Gathering and Local Prosecution of International Cybercrime. *Journal of Computer & Information Law*, 3/2002). 347.

[53] Mohamed Chawki et al.: *Cybercrime, Digital Forensics and Jurisdiction*. Springer, Cham, 2015. https://link.springer.com/book/10.1007/978-3-319-15150-2#publish-with-us.

of cybercrimes, often called the "dark side" of technology.[54] These crimes present a significant challenge for investigators and law enforcement agencies, as they must sift through vast amounts of information that require scientific analysis, such as decrypting files and breaking encrypted codes. Uncovering hidden or destroyed evidence often involves high costs and significant time and effort from expert resources that could otherwise be used more effectively in other areas.

4.6. Lack of adequate legislation and ineffectiveness where extant

Cybercrime law enforcement is hindered by inadequate legislation and ineffectiveness[55]. Out of 201 countries, only 79 have laws specifically for cybercrimes, with Western Europe being the majority[56]. This lack of laws gives cybercriminals a license to operate freely without fear. The absence of requisite laws is more prevalent in Africa, where only four countries have criminalized cybercrimes.[57] Even with existing legislation, these provisions are not severe enough to deter cybercriminals from their illegal acts[58]. Examples include Australia's Cybercrime Act 2001, Criminal Code Act 1995, and Telecommunications (Interception and Access) Act 1979.

4.7. Lack of enforcement mechanisms under international law

The paper argues that international law is not a law in practice due to its lack of enforcement mechanisms. It suggests that independence, sovereignty, and territorial bounds preserve state equality. However, the strength of nations is evident in their relations. Enforcement methods include sanctions, reciprocity, collective action, and shaming. The Budapest Convention on Cybercrime, a treaty, is an example. The non-binding nature of international law has stifled the enforcement of cybercrime laws, as states refuse to enforce provisions in their territory.

54 Richard A. Posner: *An Economic Approach to the Law of Evidence*. University of Chicago Law School, John M. Olin Law & Economics Working Paper No. 66. https://heinonline.org/HOL/LandingPage?handle=hein.journals/stflr51&div=55&id=&page=.

55 Ajayi 2016.

56 Ibid.

57 Ibid.

58 Christopher Hooper et al.: Cloud Computing and Its Implications for Cybercrime Investigations in Australia. *Computer Law & Security Review*, 2/2013, 152–163.

4.8. Weakly trained, poorly paid, and lack of protection for law enforcement agencies

This study believes that cybercriminals are crass opportunists always looking for avenues to make unlawful wealth or, in rare cases, wreak havoc on computer systems; they have been described as professional thieves and soldiers of fortune; above all, cybercriminals are experts in computers and cyberspace issues. Thus, the expertise of cyber criminals cannot be juxtaposed with law enforcement agencies, which are mere government officials who are ill-trained, poorly remunerated, and who offer their services without proper security and protection[59]. The preceding factors make efforts to investigate and enforce cybercrime laws puerile because cyber criminals are far ahead of law enforcement agencies regarding access to funds and the necessary acquisition of skills in computers and cyberspace-related issues.

4.9. Absence of one universal law governing cybercrimes

The only law explicitly dealing with international cybercrimes is the Budapest Convention, hampered by difficulties associated with international laws, an already copiously discussed issue.[60] This paper emphasizes the lack of a universal law governing cybercrimes, as they are borderless, transnational, and international crimes committed in cyberspace. Current laws and policies are fragmented due to issues such as lack of consensus on cybercrime types, definitions of criminal conduct, insufficient legal powers for investigation, lack of uniformity between national procedural laws, and absence of extradition and mutual legal assistance treaties. A universal law is needed to address these challenges.

5. Practical cases of cybercrime and electronic mail forgery that occurred in Rwanda

Cybercrime has emerged as a significant challenge in Rwanda's rapidly growing digital economy. The increasing reliance on technology in communication, business transactions, and public administration has created opportunities for cybercriminals to exploit vulnerabilities in electronic systems. Among the

[59] Ibid.
[60] Ibid.

various forms of cybercrime, electronic mail forgery is prevalent, manipulating email content, headers, or sender information to deceive recipients for financial, reputational, or other illicit gains. This section explores notable instances of cybercrime and electronic mail forgery in Rwanda, highlighting their modus operandi, legal implications, and the efforts undertaken by authorities to address these offenses. By examining these cases, the aim is to provide practical insights into the challenges of combating cybercrime and the critical role of electronic evidence in ensuring accountability and justice.

5.1. Case 1: Cyber fraud ring targeting Equity Bank

In 2020, Rwandan authorities dismantled a cybercrime syndicate attempting to infiltrate Equity Bank's systems. The group, comprising eight Kenyans, three Rwandans, and one Ugandan, sought unauthorized access to the bank's digital infrastructure to transfer funds illicitly. The Rwanda Investigation Bureau (RIB) apprehended the suspects before they could execute the heist, preventing potential financial losses and reinforcing the importance of robust cybersecurity measures in the banking sector.[61]

5.2. Case 2: Surge in cyber-fraud during COVID-19 lockdown

Between January and September 2020, Rwanda experienced a significant increase in cyber-fraud cases, with 141 incidents reported involving approximately RWF 371 million. The Rwanda Investigation Bureau (RIB) successfully recovered RWF 89 million and arrested several individuals connected to these crimes. This surge in cyber fraud, particularly during the COVID-19 lockdown, underscores the need for enhanced cybersecurity awareness and strengthened legal frameworks to combat electronic fraud effectively.[62]

[61] Rwanda Investigation Bureau, Cyber fraud scammers steal over RWF 280M in 2020. Online: https://cyber.gov.rw/updates/article/cyber-fraud-scammers-steal-over-rwf-280m-in-2020-1/.

[62] Ibid.

6. Effective Legal strategies for prosecuting and punishing cybercrime in Rwanda

This study examines various legal strategies as potential solutions to the abovementioned difficulties. Among those tactics are criminality, applying current laws, investigation, evidence gathering, prevention, and international collaboration.

6.1. Enforcement of the existing laws and conducting investigation

The United Nations code of conduct for law enforcement officials emphasizes the duty of law enforcement to serve the community and protect against illegal acts[63]. As cybercrime becomes more prevalent, law enforcement agencies must balance serving and protecting global crimes. Local police stations often transfer cases to specialized national-level leads, but electronic evidence is expected to revolutionize policing techniques. The capacity of police forces to investigate cybercrime varies between countries, with some having well-organized units and others needing more trained officers.

6.2. Increasing the power of investigation

Cybercrime evidence is typically electronic or digital, requiring a combination of traditional and new policing techniques. Law enforcement may use conventional methods, such as interviewing victims or undercover surveillance, but may also use computer-specific approaches[64]. Legal frameworks for cybercrime investigations require a clear scope of application and sufficient authority for data preservation and collection. Specialized procedural frameworks define concepts like computer data, data at rest, and data in transit and differentiate between data types like subscriber, traffic, and content data.

[63] Gerhard O. W. Mueller: The United Nations Draft Code of Conduct for Law Enforcement Officials. *Police Studies*, 2/1978.

[64] Kanae Kanki – Alexander Resch: Strengthening International Law Enforcement Cooperation. INTERPOL and Its Global Fight Against Economic and Financial Crime. In: Michala Meiselles – Nicholas Ryder – Arianna Visconti (eds.): *Corporate Criminal Liability and Sanctions*. Routledge, 2024. eBook, https://www.taylorfrancis.com/chapters/edit/10.4324/9781003324829-9/strengthening-international-law-enforcement-cooperation-kanae-kanki-alexander-resch.

6.3. Empowering Law Enforcement Capacity

This point presents information gathered on the capacity of law enforcement authorities to prevent and combat cybercrime. Institutional capacity in policing has several elements, including strategic and operational capabilities, personnel technical skills, and sufficiency of officers and resources. Another essential element of capacity is the degree of specialization. Crimes that require a specialized response typically present specific challenges in terms of offense definitions, the applicability of laws, or evidence gathering and analysis.[65] Cybercrime shows all of these characteristics, and a degree of law enforcement specialization is critical to an effective crime prevention and criminal justice response. Law enforcement specialization can occur at the organizational and personnel levels, often overlapping. While specialization will likely always be required in cybercrime and electronic evidence, it is also the case that as the world advances towards hyper-connectivity, all law enforcement officers will increasingly be expected to handle and collect electronic evidence routinely.

6.4. Increasing criminalization and respect for human rights

The increasing use of social media and user-generated internet content has resulted in regulatory responses from the government, including criminal law, and calls for respect for the right to freedom of expression[66]. International human rights law acts as a sword and a shield, requiring the criminalization of (limited) extreme forms of expression while protecting others. Some prohibitions on freedom of expression, including incitement to genocide, hatred constituting incitement to discrimination, hostility or violence, incitement to terrorism, and propaganda for war, are therefore required for states that are party to relevant international human rights instruments. The international human rights law both prescribes and prohibits criminalization in the area of cybercrime. Jurisprudence around freedom of speech is mainly developed in assisting countries to place boundaries around the criminalization of expression in areas as diverse as hate speech, incitement to terrorism, defamation, obscenity, and insult.

[65] Richard Mace: *Prosecution Organizations and the Network of Computer Crime Control. Doctoral dissertation*. 1999. AAT 9920188.

[66] Lorna Woods: User-generated content. Freedom of expression and the role of the media in a digital age. In: Merris Amos – Jackie Harrison – Lorna Woods (eds.): *Freedom of Expression and the Media*. Leiden, Martinus Nijhoff Publishers, 2012. 141-159.

A state that is a party to human rights treaties must establish criminal law and systems sufficient to deter and respond to attacks on individuals; it must not deny individual rights by criminalizing particular conduct.[67] In undertaking this assessment, the criminal law provision must be assessed on a 'right-by-right' basis to test whether its contents infringe a range of individual rights, such as the right not to be subjected to arbitrary or unlawful interference with privacy, family, home or correspondence[68], the right to freedom of thought, conscience, and religion[69], or the right of peaceful assembly.[70] International human rights law applies equally to the criminalization of cybercrime. Cybercrime represents a broad area of criminalization, including acts against the confidentiality, integrity, and availability of computer data or systems, computer-related acts for personal or financial gain or harm, and computer content-related acts. Some criminal provisions may engage international human rights law obligations more than others.

6.5. Collecting and analyzing electronic evidence through digital forensics

This point considers the criminal justice process in cybercrime cases, starting from the need to identify, collect, and analyze electronic evidence through digital forensics. It examines the admissibility and use of electronic evidence in criminal trials and demonstrates how prosecutorial challenges can impact criminal justice system performance. It links law enforcement and criminal justice capacity needs with a view of delivered and required technical assistance activities.

6.6. Increasing criminal justice capacity

Cybercrime and electronic evidence-based investigations require specialization within law enforcement; the prosecution and adjudication of cybercrime cases

67 United Nations Commission on Narcotic Drugs and Crime Prevention and Criminal Justice, 2010. Drug control crime prevention and criminal justice: A Human Rights perspective. Note by the Executive Director. E/CN.7/2010/CRP.6 – E/CN.15/2010/CRP.1. 3 March 2010.

68 ICCPR, Art. 17: International Covenant on Civil and Political Rights, Article 17 – Protection against arbitrary interference with privacy, family, home, or correspondence, and protection of honor and reputation.

69 Ibid. Art. 18.

70 Ibid. Art. 21.

also call for specialization within the criminal justice system.[71] Such specialization requires personnel who understand computing and the Internet, know cybercrime legislative frameworks, and can present and understand electronic evidence in court.

6.7. Raising cybercrime awareness

Surveys, including in developing countries, demonstrate that most individual internet users now take basic security precautions. All stakeholders highlight the continued importance of public awareness-raising campaigns, including those covering emerging threats and those targeted at specific audiences, such as children.[72] User education is most effective when combined with systems that help users securely achieve their goals.

The United Nations Guidelines for the Prevention of Crime highlight the importance of public education and awareness.[73] Increased public awareness of victimization risks and protective measures is an important strategy in preventing any crime.[74] In addition to governments, during information gathering for the Study, private sector organizations also highlighted the importance of public and corporate awareness regarding cybercrime.

6.8. International cooperation with states

A transnational dimension to a cybercrime offense arises where an element or substantial effect of the offense is in another territory or part of the modus operandi of the offense is in another territory[75]. This engages issues of sovereignty, jurisdiction, transnational investigations, extraterritorial evidence, and international cooperation requirements. Cybercrime is not the first 'new'

[71] Council of Europe, Guideline for Prosecutors and Law Enforcement in Cybercrime Investigations in Turkey, prepared by Dr. Michael Jameison and Kemal Kumkumoglu, October 2023. Available at: https://rm.coe.int/guide-on-fight-against-cybercrime/1680ae6859.

[72] Breana C. Smith – Don Ly – Mary Schmiedel: Intellectual Property Crimes. *American Criminal Law Review*, 2/2006).

[73] United Nations Guidelines for the Prevention of Crime. 2002. Economic and Security Council resolution 2002/13, Annex. Para.6 and 25.

[74] UNODC, *Handbook on the crime prevention guidelines. Making them work*. United Nations, New York, 2010. 65.

[75] UNODC, *Transnational Cybercrime: A Global Perspective*, 2020. https://www.unodc.org/documents/organized-crime/Transnational_Cybercrime_A_Global_Perspective.pdf.

crime to demand a global response. Over the past decades, global action has been required to address challenges such as illicit drug trafficking and transnational organized crime, including through the development of international agreements. Nonetheless, it has become a truism that cybercrime today presents unique international cooperation challenges.

Rules of customary public international law protect states' sovereign equality. These include states' obligations not to interfere in the internal and external affairs of other states in any form or for any reason whatsoever.[76] Law enforcement and criminal justice matters fall within the exclusive domain of the sovereign state because criminal jurisdiction has traditionally been linked to geographical territory. States must, therefore, refrain from exerting pressure on other states regarding the behavior of specific national bodies, such as law enforcement agencies or the judiciary. Persons may not be arrested, a summons may not be served, and police or tax investigations may not be mounted on the territory of another state except under the terms of a treaty or other consent given.[77] Of course, not all crimes occur neatly within the territorial jurisdiction. Where this is the case, international law has recognized several bases of extra-territorial jurisdiction in criminal matters.[78] The international cooperation of states may include cooperation through bilateral and multilateral agreements, cooperation through Jurisdiction, cooperation for gathering electronic evidence, and collaboration on extra-territorial evidence from service providers.

7. Conclusion

Cybercrime, as a phenomenon that involves the use of computers and networks to commit or facilitate offenses, presents multifaceted challenges that threaten individual, organizational, and national security. These crimes, ranging from hacking and copyright infringement to child exploitation and financial fraud, exploit modern telecommunication networks and mobile technologies to cause harm. While the global community has taken strides to address cybercrime,

[76] Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States, annex to GA resolution A/RES/20/2131 (XX), 21 December 1965. Please also refer to the Corfu Channel case, ICJ Reports 1949, 35, the Military and Paramilitary Activities case, ICJ Reports 1986, 202, and the Nicaragua case, ICJ Reports 1986, 14, 109-10.

[77] Ian Brownlie: *Principles of Public International Law*. 6th ed. Oxford, Oxford University Press, 2003. 306.

[78] Hans-Heinrich Jeschek – Thomas Weigend: *Lehrbuch des Strafrechts. Allgemeiner Teil.* 5th ed. Berlin, Duncker & Humblot, 1996. 167 et seq.

significant gaps in effective prosecution, enforcement, and prevention remain pervasive. One of the critical barriers to progress lies in the disproportionate focus on nation-state actors and their implications for national security. While these concerns are valid, this approach overshadows the increasing prevalence of financially motivated cybercrime, which affects most individuals and institutions globally. The current enforcement gap reflects insufficient attention to transnational organized cybercrime and the lack of comprehensive mechanisms for attribution, legal enforcement, and international cooperation.

Rwanda's case is emblematic of the broader challenges nations face navigating the complexities of cybercrime control in an evolving digital landscape. This paper has examined Rwanda's legal framework and enforcement mechanisms, uncovering gaps in prosecutorial effectiveness and institutional capacities. The findings underscore the urgent need for reform to strengthen legal provisions, enhance investigative tools, and foster capacity-building initiatives for law enforcement agencies.

To reverse the enforcement gap, a unified approach that aligns national and international stakeholders on shared priorities is required. This includes establishing frameworks to tackle transnational cybercrime networks, eliminating safe havens for perpetrators, and fostering collaboration between governments, corporations, and international organizations. Investing in technological capabilities, harmonizing legal standards with international conventions, and fostering judicial and law enforcement expertise will be critical steps forward for Rwanda and other nations.

As technology evolves, emerging threats will further test the resilience of national and global cybercrime control mechanisms. Rwanda's experience highlights the importance of proactive legal and institutional responses to prevent cybercrime from reaching epidemic proportions. By integrating lessons learned through comparative analysis and collaboration with international partners, Rwanda can position itself as a model for addressing cybercrime in developing contexts.

Addressing cybercrime requires a long-term vision emphasizing prevention, cooperation, and adaptability to technological advancements. The global community must embrace shared values and principles to reduce the enforcement gap and ensure the digital landscape remains secure for all. For Rwanda, leveraging its unique context and experiences can drive impactful reforms contributing to national security and regional and global cybersecurity resilience.

Bibliography

Richard Anderson et al.: "Measuring the Changing Cost of Cybercrime". Paper presented at The 18th Annual Workshop on the Economics of Information Security (WEIS 2019), Boston, 2019. https://weis2019.econinfosec.org/program/agenda/.

John Aycock: *Computer Viruses and Malware.* New York, Springer Science & Business Media, 2006.

M. Cherif Bassiouni: *The Sources and Content of International Criminal Law. A Theoretical Framework*. Leiden, Martinus Nijhoff Publishers, 1999.

Cameron Scott Doran Brown: Investigating and Prosecuting Cyber Crime. Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, 1/2015, 55–119. Available at: https://cybercrimejournal.com/pdf/Brown2015vol9issue1.pdf.

Samuel W. Buell: What Is Securities Fraud. *Duke Law Journal*, 3/2011, 511–581.

Thomas M. Chen – Jean-Marc Robert: The Evolution of Viruses and Worms. In: William W.S. Chen (ed.): *Statistical Methods in Computer Security*. Boca Raton, CRC Press, 2004. 289-310. https://www.taylorfrancis.com/chapters/edit/10.1201/9781420030884-19/evolution-viruses-worms-thomas-chen-jean-marc-robert.

Christopher, Rocks. „Extradition, Human Rights, and the Death Penalty: When Nations Must Refuse to Extradite a Person Charged with a Capital Crime." California Western International Law Journal, 25 (1994): 189. https://heinonline.org/HOL/LandingPage?handle=hein.journals/calwi25&div=10&id=&page=

Craig R. Roecks: Extradition, Human Rights, and the Death Penalty. When Nations Must Refuse to Extradite a Person Charged with a Capital Crime. *California Western International Law Journal*, 1/1994. https://heinonline.org/HOL/LandingPage?handle=hein.journals/calwi25&div=10&id=&page=.

Choo, Kim-Kwang Raymond. „Online Child Grooming: A Literature Review on the Misuse of Social Networking Sites for Grooming Children for Sexual Offences." Australian Institute of Criminology (2009). https://www.aic.gov.au/sites/default/files/2020-05/rpp103.pdf.

Kim-Kwang Raymond Choo: *Online Child Grooming. A Literature Review on the Misuse of Social Networking Sites for Grooming Children for Sexual Offences*. Canberra, Australian Institute of Criminology, 2009. https://www.aic.gov.au/sites/default/files/2020-05/rpp103.pdf.

Sumanjit Das – Tapaswini Nayak: Impact of Cyber Crime. Issues and Challenges. *International Journal of Engineering Sciences & Emerging Technologies*, 2/2013, 142–153. Available at: https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf.

Emmanuel Ajayi: Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, 1/2016, 1–12. https://www.researchgate.net/

publication/307528405_Challenges_to_enforcement_of_cybercrimes_laws_and_policy.

John Gacinya: *Criminal Justice System as an Instrument of Internal Security. A Case Study of Rwanda. Master's thesis*. Institute of Diplomacy and International Studies (IDIS), University of Nairobi, 2013. 75-159. https://erepository.uonbi.ac.ke/bitstream/handle/11295/166148/Criminal%20Justice%20System%20as%20an%20Instrument%20of%20Internal%20Security%20a%20Case%20Study%20of%20Rwanda.pdf?sequence=1.

Roger Généreux Ishimwe: *Critical analysis on the impact of cybercrimes on intellectual property rights under Rwanda legal framework*. Kigali Independent University ULK, 2024. http://drepository.ulk.ac.rw:8080/xmlui/bitstream/handle/123456789/362/CRITICAL%20ANALYSIS%20ON%20THE%20IMPACT%20OF%20CYBERCRIMES.pdf?sequence=1&isAllowed=y.

Hamid Jahankhani – Ameer Al-Nemrat – Amin Hosseinian-Far: Cybercrime Classification and Characteristics. In: Babak Akhgar – Andrew Staniforth – Francesca Bosco (eds.): *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Waltham, Syngress, 2014. 149–164.

Anja P. Jakobi: Non-State Actors All Around. The Governance of Cybercrime. In: Anja P. Jakobi – Klaus Dieter Wolf: *The Transnational Governance of Violence and Crime. Non-State Actors in Security*. London, Palgrave Macmillan, 2013. 129–148.

Kanae Kanki – Alexander Resch: Strengthening International Law Enforcement Cooperation. INTERPOL and Its Global Fight Against Economic and Financial Crime. In: Michala Meiselles – Nicholas Ryder – Arianna Visconti (eds.): *Corporate Criminal Liability and Sanctions*. Routledge, 2024. eBook, https://www.taylorfrancis.com/chapters/edit/10.4324/9781003324829-9/strengthening-international-law-enforcement-cooperation-kanae-kanki-alexander-resch.

Mace, Richard. Prosecution Organizations and the Network of Computer Crime Control. Doctoral dissertation, 1999.

Richard Mace: *Prosecution Organizations and the Network of Computer Crime Control. Doctoral dissertation*. 1999. AAT 9920188.

William Maluleke: Exploring Cybercrime. An Emerging Phenomenon and Associated Challenges in Africa. *International Journal of Social Science Research and Review*, 6/2023, 223–243.

John Reid Meloy: Stalking. An Old Behavior, A New Crime. *Psychiatric Clinics of North America*, 1/1999, 85–99. https://www.sciencedirect.com/science/article/abs/pii/S0193953X05700617.

Fidelis Chukwunenye Obodoeze: "Cyber Crimes. Effects of Information Technology and Globalization on World Economy." Paper presented at the UNESCO World Philosophy Day Celebration Workshop, Nnamdi Azikiwe University, Awka, Nigeria,

November 21-23, 2011. https://www.researchgate.net/publication/340333512_CYBER_CRIMES_EFFECTS_OF_INFORMATION_TECHNOLOGY_AND_GLOBALIZATION_ON_WORLD_ECONOMY.

Emmanuel O. C. Obidimma – Richard Onyekachi Ishiguzo: Cybercrime Investigation and Prosecution in Nigeria. The Critical Challenges. *African Journal Of Criminal Law And Jurisprudence*, 8/2023, 30–36.

Michael Pittaro: Cyberstalking. An Analysis of Online Harassment and Intimidation. *International Journal of Cyber Criminology*, 2/2007, 180–197.

Richard A. Posner: *An Economic Approach to the Law of Evidence*. University of Chicago Law School, John M. Olin Law & Economics Working Paper No. 66. https://heinonline.org/HOL/LandingPage?handle=hein.journals/stflr51&div=55&id=&page=.

Robert J. Sciglimpaglia, Jr.: Computer Hacking. A Global Offense. *Pace Yearbook of International Law*, 1/1991, 199–266. https://digitalcommons.pace.edu/pilr/vol3/iss1/.

Zunaira Sattar et al.: "Challenges of Cybercrimes to Implementation of Legal Framework." Paper presented at the International Conference on Emerging Technologies, November 1, 2018. https://www.semanticscholar.org/paper/Challenges-of-Cybercrimes-to-Implementation-of-Sattar-.

David S. Wall – Majid Yar: Intellectual Property Crime and the Internet. Cyber-Piracy and 'Stealing' Information Intangibles. In: Yvonne Jewkes – Majid Yar (eds.): *Handbook of Internet Crime*. 2nd ed., Oxford, Routledge, 2011. 230-255.

Peter A. Winn: The guilty eye. Unauthorized access, trespass, and privacy. *The Business Lawyer*, 4/2007, 1395–1437.

HISTORY OF FORMATION AND DEVELOPMENT OF CONSTITUTIONAL CONTROL IN THE REPUBLIC OF KAZAKHSTAN

Bayan Oshan[1]

ABSZTRAKT ■ Ez a tanulmány részletes feltárást kínál a Kazah Köztársaság alkotmányos ellenőrzésének történetéről, kialakulásáról és fejlődéséről.. A jogi keretrendszer részleteibe mélyedve a tanulmány több kulcsfontosságú altémán keresztül bontakozik ki. Először is megvizsgálja a kazah alkotmányos kontrollmechanizmusok fejlődési pályáját, nyomon követve fejlődésüket a kezdetektől a mai szerkezetükig. Másodsorban elemzi az Alkotmánytanács kulcsszerepét a nemzeten belüli alkotmányos ellenőrzés kialakításában és előmozdításában. Különös hangsúlytkap a tanács funkcióinak, hatáskörének és az ország jogi környezetéhez való hozzájárulásának megvilágítása.. A tanulmány megvizsgálja továbbá a kazah bíróságok fellebbezéseire válaszul indított alkotmányos eljárások sajátosságait, kiemelve az ebben a folyamatban rejlő árnyalatokat és kihívásokat. Végül górcső alá veszi az Alkotmánybíróság kialakulásának szakaszait és intézményi felállítását, betekintést nyújtva annak történelmi összefüggéseibe és jelentőségébe. Ezen altémák alapos vizsgálata révén ez a cikk átfogó képet nyújt az alkotmányos ellenőrzés dinamikus fejlődéséről a Kazah Köztársaságban,, rávilágítva annak jogi keretrendszerére, intézményi mechanizmusaira, valamint a kormányzásra és a jogállamiságra gyakorolt szélesebb körű hatásaira.

ABSTRACT ■ This paper offers a thorough exploration of the history, formation, and progression of constitutional control within the Republic of Kazakhstan. Delving into the intricacies of this legal framework, the study unfolds through several key subtopics. Firstly, it examines the developmental trajectory of constitutional control mechanisms in Kazakhstan, tracing their evolution from inception to their contemporary structure. Secondly, it analyzes the pivotal role played by the Constitutional Council in shaping and advancing constitutional control within the nation. Special emphasis is placed on elucidating the council's functions, powers, and contributions to the country's legal landscape. Furthermore, the paper investigates the specifics of constitutional proceedings initiated in response to appeals from courts across Kazakhstan, highlighting the nuances and challenges inherent in this process. Lastly, it scrutinizes the formative stages and institutional establishment of the Constitutional

[1] PhD Student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

Court, providing insights into its historical context and significance. Through a meticulous examination of these subtopics, this article offers a comprehensive understanding of the dynamic evolution of constitutional control in the Republic of Kazakhstan, shedding light on its legal framework, institutional mechanisms, and broader implications for governance and rule of law.

Keywords: constitution, constitutional control, constitutional court

1. Introduction

The establishment of constitutional control in the Republic of Kazakhstan relates to the constitutional establishment of the formation of a state based on the rule of law. The unconditional supremacy of the Constitution over other normative acts is one of the features of a state based on the rule of law. Another fundamental principle of the rule of law is the supremacy of law, which is expressed in the mandatory subordination of the state itself and its bodies to the Constitution of the Republic of Kazakhstan.

Constitutional control is a special type of law enforcement activity in the state, which consists in checking the compliance of laws and other normative acts with the constitution of a given country. The institution of constitutional control is the power granted to the people appointed to it to control and, if necessary, to sanction the conformity to the constitution of acts adopted by public authorities and especially of laws voting by representatives elected by the sovereign people.[2]

The main mission of constitutional control is to ensure the supremacy and stability of the constitution, to preserve the constitutional separation of powers and to guarantee the protection of constitutionally enshrined human rights and freedoms. In addition, one of the important functions of constitutional justice is to control the constitutionality of normative legal acts of various types.

Testing for constitutionality is a way to resolve conflicts generated by contradictions between normative acts of different legal forces. The necessity of hierarchical order in the legal system causes the need to control the conformity of acts of national legislation and international obligations of the state.

In the Republic of Kazakhstan, the following groups of normative legal acts are subject to control for compliance with the Constitution: laws adopted by the

[2] B. I. Ismailov: "The formation of a system of constitutional control in the law enforcement practice of foreign states." In: *All-Russian digital encyclopedia*. Portalus, Moscow, 2008.

Parliament; resolutions adopted by the Parliament and its Chambers; international treaties of the Republic before their ratification.[3]

2. Development of constitutional control in Kazakhstan

According to Mukanov K., the periodisation of the development of constitutional control in the Republic of Kazakhstan is directly related to the periods of state-legal development of Kazakhstan.[4]

The first period comprises the largest time period, which includes the stages of formation of constitutionalism of Kazakhstan, starting from the Kazakh khanate to independence, including the entire Soviet period.

The second period is marked by the acquisition of sovereignty as a result of the collapse of the USSR, the adoption of the Constitution of the Republic of Kazakhstan in 1993 and on its basis the creation of the country's valid practising body of constitutional control – the Constitutional Court that was the first in its history until its disbanding.

The third period shows a new form of constitutional justice in Kazakhstan – the Constitutional Council, which was formed on the basis of the Constitution of the Republic of Kazakhstan adopted at the republican referendum on 30 August 1995.

A number of scientific studies by scholars in Kazakhstan indicate that the first stage includes the post-revolutionary period of the 20th century, having in mind the programme acts of the "Alash autonomy" adopted at that time. For example, such acts as a set of rules of customary law called "Char Provision" of 1885, "The Bright Way of Kasym Khan", "The Old Way of Esim Khan", Seven Regulations of Tauke Khan ("Zhety Zhargy") became a kind of the beginning of the formation of Kazakh constitutionalism, and its continuation is the entire Soviet period, when the prerequisites for the introduction of institutions of constitutional control matured and articulated, but in fact this control was not institutionalised.

The establishment and creation of a specialised body of constitutional control became possible only in the early 1990s, after the collapse of the USSR and, accordingly, the abandonment of the Soviet legal ideology, which denied the need to protect the Constitution. On 22 September 1989, the Supreme Soviet of the Kazakh SSR made amendments and additions to the Constitution (the Basic Law)

[3] А. И. Зыбайло: Конституционный контроль и международные обязательства государств. In: *Вестник Института законодательства Республики Казахстан*. – № 4 (24). Almaty, 2011. 197.

[4] К. М Муканова: Становление и развитие института конституционного контроля в РК. ББК 74.58 М 75, 182.

of the Kazakh SSR in order to develop socialist democracy and improve the bodies of justice. One of the progressive amendments made to the Constitution was the addition providing for the establishment of the Committee of Constitutional Supervision of the Kazakh SSR. The Committee of Constitutional Supervision was vested with the following powers: to submit to the Supreme Soviet of the Kazakh SSR an opinion on the conformity of acts of the Supreme Soviet with the Constitution and laws of the Kazakh SSR; to monitor the conformity of resolutions and orders of the Council of Ministers, decisions of local Soviets of People's Deputies with the Constitution and laws of the Kazakh SSR; to give an opinion on the conformity of acts of other state bodies and public organisations with the Constitution and laws of the Kazakh SSR.

Final decisions adopted by the Constitutional Supervision Committee did not have binding legal force for those subjects who adopted acts not corresponding to the Constitution and laws of the Kazakh SSR. Final decisions of the Constitutional Supervision Committee could be implemented only after elimination of contradictions by the same body that adopted acts not corresponding to the Constitution and laws of the Kazakh SSR. The Committee of Constitutional Supervision in case of detection of contradictions could only suspend the execution of unconstitutional acts. The cancellation of such acts was the prerogative only of the Supreme Soviet or the Council of Ministers, where the Committee of Constitutional Supervision should enter with a submission on the cancellation of acts not corresponding to the Constitution and laws of the Kazakh SSR.[5]

The Law "On Amendments and Additions to the Constitution of the Kazakh SSR" also provided for the order of formation of the composition, the status of persons elected to the Committee of Constitutional Control. However, in accordance with this normative legal act, the Committee of Constitutional Supervision was not the only body of constitutional control. These amendments also entrusted the Presidium of the Supreme Soviet of the Kazakh SSR with control over the observance of the Constitution of the Kazakh SSR.

Constitutional amendments to establish a Constitutional Oversight Committee were ultimately not implemented. The Constitutional Review Committee of the Republic, unlike the Union Constitutional Review Committee, was not established. The lofty intentions of the Constitution remained only on paper. The creation of the Committee was hindered by various reasons, including the unpreparedness of the party-bureaucratic power structure for new political and legal transformations and the recognition of the priority of law.

[5] И. И. Рогово – В. А. Малиновского: *Конституционный контроль в Казахстане. Доктрина и практика утверждения конституционализма*. Almaty, 2015. 85.

After gaining sovereignty and subsequent independence, the Republic of Kazakhstan embarked on the difficult path of forming a new type of statehood. In this regard, the Constitutional Law of 16 December 1991 "On the State Independence of the Republic of Kazakhstan" was of particular importance, Article 10 of which immediately designated the highest body of judicial protection of the Constitution – the Constitutional Court of the Republic of Kazakhstan.

Two constitutional laws became an indicative achievement of numerous debates and disputes concerning the form and structure of the formation of the Court, its set of powers, rights and duties, and the competence of the final acts: the Law of the Republic of Kazakhstan dated 5 June 1992 "On the Constitutional Court of the Republic of Kazakhstan" and "On Constitutional Court Proceedings in the Republic of Kazakhstan". The competence of the Constitutional Court consisted of control over the compliance with the Constitution of the Republic of Kazakhstan of the following normative legal acts:

- laws and other acts adopted by the Supreme Soviet;
- decrees and other acts of the President;
- decrees of the Cabinet of Ministers;
- normative acts of ministries, state committees and departments;
- normative acts of the Prosecutor General of the Republic of Kazakhstan, guiding explanations of the Supreme and Supreme Arbitration Courts of the Republic of Kazakhstan;
- international treaties and other obligations of the Republic of Kazakhstan that have not entered into force.

The competence of the Court also included consideration of cases on verification of the constitutionality of law enforcement practices affecting the constitutional rights of citizens.

However, it is important to note that the Constitutional Court of the Republic of Kazakhstan did not have competence to resolve issues that traditionally fall within the competence of European constitutional courts. For example, the Constitutional Court of the Republic of Kazakhstan, unlike the Constitutional Court of the Italian Republic, did not have the authority for preliminary constitutional control of constitutional amendments to the Constitution, submitted to referendum, and the authority to check the constitutionality of the procedure and results of the referendum itself.

At the same time, the role and practice of the Constitutional Court in the history of the formation of constitutional control of the Republic of Kazakhstan is important. To ensure constitutional legality and supremacy of the Constitution, disputes on the conformity to the Constitution of the Republic of Kazakhstan

of acts of state bodies, actions of its highest officials, as well as the practice of application of constitutional legislation of the Republic of Kazakhstan were resolved, which laid the foundation for constitutional control in the state.

Thus, it can be concluded that the activity of the Constitutional Court of the Republic of Kazakhstan was well within the European legal context of constitutional control, but the reasons for the abolition of this body lie outside the legal theory.

The Constitution of the Republic of Kazakhstan, adopted at the republican referendum on 30 August 1995, established a new body of constitutional control – the Constitutional Council of the Republic of Kazakhstan, in connection with which the Constitutional Court was abolished.

Regarding the opinion of the first president, the stability of state institutions was especially important, when Kazakh society is at the initial stage of democratization. Therefore, the establishment of a constitutional justice body exercising subsequent control over the constitutionality of laws, elections, as some believed, is fraught with negative consequences and carries a threat to political stability. The French model of constitutional justice – the Constitutional Council, which exercises preliminary control over the observance of the norms of the Constitution, does not have the right to independently initiate cases and does not consider specific judicial disputes – is more acceptable for transitional societies.

The Concept of Forming the State Identity of the Republic of Kazakhstan, approved by the Order of the President of the Republic of 23 May 1996, states that the Constitution of the country provides for such a state body as the Constitutional Council. Under the conditions of presidential rule, when the President is the supreme arbiter in the state, the Constitutional Council serves as the optimal model of a body to ensure constitutional legality.

The year 2022 brought a new turn in the history of Kazakhstan. The first article of the Law "On Amendments and Additions to the Constitution of the RK" states that the word "council" is changed to "court". Since the amendments were adopted, the Constitutional Court was restored in Kazakhstan from 1 January 2023.

3. The role of the constitutional council in the development of constitutional control in Kazakhstan

Since the Constitutional Court was restored in an inconsistent manner, to understand the development of constitutional control in Kazakhstan, it is necessary to analyse the Constitutional Council.

The Constitutional Council consisted of seven members. The Chairman and two members of the Council are appointed by the President of the Republic, two members each are appointed by the Senate and Majilis of Parliament for a term of six years. Half of the members of the Council are renewed every three years. In addition, ex-Presidents of the Republic are by right members of the Constitutional Council for life.

The legal basis for the organisation and activities of the Council is the Constitution and Constitutional Act No. 2737 of 29 December 1995 on the Constitutional Council of the Republic of Kazakhstan. According to its constitutional status, the Council, in exercising its powers, is autonomous and independent of State bodies, organisations, officials and citizens, subject only to the Constitution of the Republic and may not proceed from political or other motives.

The Constitution of the Republic establishes the range of powers of the Constitutional Council, including: in the event of a dispute, deciding on the correctness of the elections of the President of the Republic, deputies of Parliament and the holding of a republican referendum; reviewing laws adopted by Parliament for their conformity with the Constitution of the Republic before the President signs them; reviewing international treaties of the Republic for their conformity with the Constitution before they are ratified; officially interpreting the norms of the Constitution; giving opinions in the cases envisaged in paragraphs 1 and 2 of the Article 1 of the Constitution; issuing opinions in the cases envisaged in paragraphs 1 and 2 of the Constitution.

Constitutional proceedings may be initiated only on appeals of the President of the Republic of Kazakhstan, Chairpersons of the Chambers of Parliament, at least one fifth of the total number of deputies of Parliament, and the Prime Minister.

The subjects of appeal to the Constitutional Council did not include citizens of the Republic. Their constitutional rights and freedoms may be protected in the courts of general jurisdiction and before the Constitutional Council in the cases and in accordance with the procedure established by article 78 of the Constitution, according to which, if a court finds that a law or other normative legal act subject to application infringes on the human and civil rights and freedoms enshrined in the Constitution, it must suspend proceedings and apply to the Constitutional Council to declare the act unconstitutional.

The constitutional reforms carried out in the country have played an important role in the development of the institution of constitutional review.

In 2007, resolutions adopted by Parliament and its chambers were subject to review by the Constitutional Council.

By way of a legislative initiative of the President of the Republic of Kazakhstan, in 2008 additions were made to the Constitutional Council Constitutional Act, under which recommendations and proposals for improving legislation contained in decisions of the Constitutional Council are subject to mandatory consideration by the authorised State bodies, with mandatory notification of the Constitutional Council of the decision taken.

4. Specifics of constitutional proceedings initiated on appeals of courts of the Republic of Kazakhstan

The legal positions of the Constitutional Council of the Republic of Kazakhstan were divided into the following groups:

- on the issues of modernisation of the constitutional doctrine of the Republic of Kazakhstan;
- on the consolidation and guarantee of the foundations of the constitutional system of the Republic of Kazakhstan, on the strengthening of a legal, democratic and social state in Kazakhstan;
- on strengthening the mechanism of protection of human and civil rights and freedoms;
- on improvement of the electoral system of the Republic of Kazakhstan;
- on the development of sectoral legislation of the Republic of Kazakhstan.

It should be noted that legal positions acquired a generally binding character through their reflection in the normative resolutions of the Constitutional Council of the Republic of Kazakhstan. It is the generally binding nature of the legal positions of the Constitutional Council that gave its decisions the force of sources of law. Legal positions of the Constitutional Council are binding not only for law enforcement bodies, but also for legislative bodies. Many legal positions served as a reference point for the legislator; he is obliged to take the position into account in new regulation and may not re-adopt a norm of the same content and meaning that was recognized as unconstitutional.

Such a feature of legal positions as their generally binding nature is of particular importance in matters of protection, guaranteeing and ensuring human and civil rights and freedoms.[6]

[6] Zaure Ayupova: Constitutional Liberties in the Republic of Kazakhstan. *Tulsa Journal of Comparative and International Law*, 1/1998, 77–86.77.

Thus, analysing the specificity of legal positions in the decisions of the Constitutional Council of the Republic of Kazakhstan on the protection of fundamental rights and freedoms of citizens of the republic, as far back as in 2005 in his dissertation research Ostapovich I.Y. noted that *"fundamentally important decisions were taken by the Constitutional Council when considering cases on individual constitutional human rights and freedoms. The analysis of its decisions related to pension legislation, legislation on employment, social security and benefits to certain categories of citizens showed that the Constitutional Council contributes to the harmonisation of legislation with the Constitution"*.[7] Noting the correctness of this statement, it should be noted that from 2005 to 2017 the Constitutional Council adopted a significant number of decisions on the protection of citizens' rights, including those initiated by the courts of the Republic.

Since the citizens of the Republic of Kazakhstan did not have the right to appeal directly to the Constitutional Council for the protection of their rights, the body of constitutional control acquires special importance in the issue of protection of their constitutional rights and freedoms. Consequently, it can be concluded that citizens have the right to initiate consideration of the unconstitutionality of a law or other legal act infringing their rights in the Constitutional Council through the courts. Accordingly, there is a link between citizens of the Republic of Kazakhstan and the body of constitutional control through the system of courts of the country.

The link is made through the consideration of specific cases on the recognition of acts of sectoral current legislation as unconstitutional. When considering specific cases and making decisions on them, the Constitutional Council reflects in them its legal positions aimed at protecting and ensuring the Fundamental Law of the country, which are a reflection of the constitutional and legal doctrine existing in this state, including the ideas and theories laid down in the Constitution, the provisions of the Constitution and the state legislation based on it, as well as the whole complex of instruments for the implementation of these provisions in life, their legal support, guarantee and implementation.

The analysis of the decisions adopted by the Constitutional Council during the period of its activity has shown that on applications of the courts, cases have been considered in the following areas of life activity of the individual, society and the state:

1) relations in the sphere of migration policy – 1 judgement;

2) relations in the area of civil law – 3 judgements;

[7] И. Ю. Остапович: *Конституционный Совет Республики Казахстан. Вопросы теории и практики*. Томск, 2005. 92.

3) relations in the area of civil procedural relations – 2 judgements;
4) relations in the sphere of social protection of the population – 3 decisions;
5) relations in the sphere of regulation of the Criminal Code of the Republic of Kazakhstan and the Criminal Procedure Code of the Republic of Kazakhstan – 7 decisions;
6) in the sphere of notaries – 1 decision;
7) in the sphere of administrative and legal relations – 4 decisions;
8) in the sphere of legal regulation of the status of arbitration courts on economic disputes – 1 decision;
9) on the issues of amnesty – 1 decision;
10) in the sphere of advocacy – 2 decisions;
11) in the sphere of taxation – 1 decision;
12) on issues of legal regulation of the civil service – 1 decision;
13) on issues of legal regulation of the status of the Baikonur complex – 1 decision;
14) on issues of religion – 1 decision.

An example is the decision of the Constitutional Council of the Republic of Kazakhstan, which *"declared unconstitutional the provisions of the Act on amendments and additions to certain legislative acts of the Republic of Kazakhstan on freedom of religion and religious associations"*. In its Resolution No. 1 of 11 February 2009, the Constitutional Council stated that the Act, in terms of the possibility of restricting "freedom to manifest religion", was inconsistent with paragraph 3 of article 39 of the Constitution. The purposes listed in the norm of the Law, for the achievement of which the possibility of such a restriction is allowed, are expanded in comparison with the constitutionally significant purposes named in paragraph 1 of Article 39 of the Constitution, and do not coincide with them.[8]

Such diversity of covered spheres of legal relations shows that the legislation should be developed in a timely manner, keeping up with the daily progressing needs of society in different spheres of its life activity, which is not always the case. It should be noted that the range of relations regulated by the norms of Kazakh law is constantly expanding. With the development of the economy, social sphere, international relations, science, development and implementation of new technologies, business, etc., there are new spheres of relations that require legal intervention. In 2016-2017 alone, the Parliament adopted more than 100 laws, which is caused by the development of legal relations in the sphere of

[8] И. И. Рогова – А. К. Котова: *Конституционный контроль в Казахстане*. Алматы, 2005. 232.

bringing the republican constitutional and legal legislation into compliance with the new version of the Constitution, is connected with the development of free economic zones in the Republic of Kazakhstan, the introduction of new medical, reproductive, food, pharmaceutical, cosmetic, cosmetic, agrarian, environmental, processing, energy, logistics, transport, customs, tax and other technologies, the emergence of new technologies, and the introduction of new technologies.

The special attention of the country's leadership, the Government and the entire Kazakh community is drawn to the issues of combating such a social evil as corruption, especially in the sphere of providing public services to the population, protecting and ensuring human rights. *"In the process of improving legislation and law enforcement activities, it is necessary to steadfastly follow the principles of the supremacy of the Constitution and compliance of lower-level acts with higher-level acts. Systemic measures are needed to ensure both the regime of legality in the country and the stability of the legal system, as well as the progressive development of national law within the framework of the current Constitution. An integrated approach to legal policy will allow us to modernise the entire legal and regulatory framework in the context of the overall strategy for the development of the state, including the construction of a qualitatively new model of public administration on the principles of efficiency, transparency and accountability, ensuring the protection of the rights and freedoms of citizens, the interests of society and the state"*.[9]

Many legislative acts are adopted in the history of Kazakhstan for the first time, and many of their provisions in the process of law enforcement practice may be tested painfully and for a long time and are likely to cause disputes and conflict situations that will be considered by the courts and serve as a basis for the courts to appeal to the Constitutional Council. Consequently, the range of public relations on which the Constitutional Council will take decisions will increase and expand. In addition, with the establishment and work of special courts in Kazakhstan, such as juvenile, administrative, economic, financial, mediation, etc., the number of cases to be considered and, accordingly, the range of potential subjects of appeals will expand. Accordingly, the number of appeals to the Constitutional Council will increase significantly, and the load on the members of the Constitutional Council will also increase, which will require them to improve their professional qualities, special knowledge and strengthen their legal positions.[10]

[9] Указ Президента Республики Казахстан, О Концепции правовой политики Республики Казахстан на период с 2010 до 2020 года» от 24 августа 2009 года, № 858 // https://online.zakon.kz/Document/?doc_id=30463139. 05.12.2017.

[10] Jakub Jakusik: Constitutional Reforms and the Circumstances Behind the Transition of Power in the Republic of Kazakhstan. In: Gulayhan Aqtay – Cem Erdem (eds.): *Language and Society in Kazakhstan. The Kazakh Context*. Poznań, Adam Mickiewicz University, 2020. 59-70. 59.

The institution of consideration by the Constitutional Council of the Republic of Kazakhstan of appeals of courts on the constitutionality of laws and other legal acts traces the connection and determination of the balance between the legal positions of the Parliament as a legislative body, courts as direct law enforcers and the Constitutional Council of the country as an interpreter of the Constitution and the supreme arbiter of the constitutionality of all acts. This is the essence and significance of the institution of consideration by the Constitutional Council of the Republic of Kazakhstan of appeals by the courts on the constitutionality of laws and other legal acts. The Constitutional Council, when resolving a clash between the legal positions of the court and the legal positions of the legislator, becomes a real official force endowed with the right to resolve the problem of the correlation of the strength of these positions, and reflects in its decision the spirit and letter of the Constitution as an act that embodies the will of the people of Kazakhstan. In the decisions of the Constitutional Council its own legal positions aimed at protecting and ensuring the interests of the citizens of Kazakhstan, civil society, legal, democratic and social state are honed.

From the point of view of relations between an individual citizen and the body of constitutional control in Kazakhstan, in fact, this institution is the only opportunity for a citizen to indirectly raise the issue of checking the compliance with the Constitution of an act that is applied to him, his rights, freedoms, duties, family, property, honour, dignity and other vital interests and which, possibly, violates them.

It should be remembered that *"one of the important mechanisms for ensuring the regime of constitutional legality, accurate interpretation of the principles and norms of the Constitution, formation of guidelines for the development of national law and law enforcement practice is to increase the effectiveness of the Constitutional Council and the exhaustive practical implementation of its normative decisions in the legal policy of the state. In the process of further establishing the principles of the rule of law in the country, it is important, on the one hand, to ensure that the exercise of constitutional human and civil rights and freedoms is guaranteed to the greatest extent possible and, on the other hand, that all State bodies, officials, citizens and organisations fulfil their constitutional obligations unconditionally and exhaustively. To ensure human and civil rights and freedoms, it is important to create conditions that guarantee equality of rights and freedoms regardless of origin, social, official and property status, sex, race, nationality, language, attitude to religion, beliefs, place of residence or any other circumstances, as required by our Constitution"*.

Legal positions of the Constitutional Council are reflected in the annual Message "On the state of constitutional legality in the Republic of Kazakhstan", which is announced at a joint session of the Chambers of the Parliament of the

Republic of Kazakhstan. The messages of the Constitutional Council have been adopted since 1996 and contain analyses as well as proposals for strengthening constitutional legality. Throughout all the years in which the Constitutional Council has been issuing its annual messages, it has kept its attention focused on the protection and safeguarding of the rights and freedoms of citizens, considering, among other things, cases on applications from the courts. Thus, already in its first Address "On the State of Constitutional Legality in the Republic of Kazakhstan" (based on the results of its work for 1996) it was noted that *"during the first year of its work, the Constitutional Council considered 11 appeals: 2 – on the constitutionality of laws adopted by the Parliament, 4 – on issues of official interpretation of the norms of the Constitution and 5 – on appeals of the courts of the Republic"*.[11]

Touching upon such an important issue as infringement of human and civil rights and freedoms, the constitutional review body emphasises that in the first year of its existence, the Constitutional Council also faced the fact that some courts in their submissions proceed from a very common interpretation of legal acts infringing human and civil rights and freedoms. Thus, the chairman of the East Kazakhstan regional court addressed the Constitutional Council with a submission to recognise article 19 of the Law of the Republic of Kazakhstan "On Trade Unions" unconstitutional, according to which dismissal on the initiative of the administration of employees elected to trade union bodies is not allowed within two years after the end of the elected powers, except in cases of complete liquidation of the enterprise or the employee's culpable actions. In the opinion of the chairman of the court, the above article of the Law contradicts the provisions of Article 14 of the Constitution of the Republic of Kazakhstan that all are equal before the law and the court.

In refusing to accept the submission, the Constitutional Council proceeded from the fact that the infringement of human and civil rights and freedoms should be referred to only in cases where the laws establish worse conditions for certain individuals or an insignificant group of them than for the bulk of the population. If the laws refer to benefits and advantages of individual or a group of subjects, which may to some extent worsen the situation of the bulk of the population, the validity of such benefits and advantages can be challenged in accordance with the established procedure.

In the Message, the Constitutional Council, formulating its legal positions, notes that *"some appeals were caused by the fact that previously adopted laws conflict with the norms of the Constitution. Therefore, it is necessary to bring legislation into*

[11] Послание Президента Республики Казахстан Н. Назарбаева народу Казахстана от 31 января 2017 года Третья модернизация Казахстана: глобальная.

line with the current Constitution (Article 92). Execution of the Constitution and laws is a necessary and constant rule of life, therefore, bringing laws into compliance with the Constitution is an important stage in ensuring compliance with constitutional legality".

This statement reflects the realities of the second half of the 90s, the stage of formation and strengthening of the sovereignty and statehood of Kazakhstan, the formation of an array of its own constitutional, legal and other sectoral legislation, the creation of its own professional apparatus of public administration, as well as the beginning of the formation of state ideology, Kazakh patriotism and the beginning of the formation civil society. All this, based on the provisions of the Constitution of the Republic of Kazakhstan, relying on the achievements of domestic and foreign constitutional and legal science, created the basis for the formation and strengthening of the legal position of the Constitutional Council, including on appeals from the courts of the republic.[12]

Subsequently, over the years of strengthening the independence of Kazakhstan, in the process of qualitative changes in the political, social and economic life of the country, carrying out deep reforms that affected all aspects of the life of Kazakh society, in connection with changes in the development of legislation and law enforcement practice of the republic, the current tasks facing the Constitutional Council are changing, during these years, constantly resolving cases on appeals from the courts of the Republic of Kazakhstan.

But the main tasks of the constitutional control body to protect the rights and freedoms of citizens remain unchanged and paramount, which is repeatedly emphasized in the Messages of the President of the Republic to the people of Kazakhstan. In his Message dated January 31, 2017, the Head of State noted that all the achievements of the Kazakh people over the years of their independence *"are the result of the correct political path and the high authority of Kazakhstan in the international arena. Kazakhstan should be among the 30 developed countries of the world by 2050. We are confidently moving towards this goal".*[13]

In its Messages over the years of independence, the Constitutional Council of the Republic of Kazakhstan constantly focuses on the establishment of constitutionalism in the Republic of Kazakhstan, strengthening constitutional legality, rights and freedoms of citizens, using various institutions.

[12] Alexei Trochev – Alisher Juzgenbayev: Instrumentalization of constitutional law in Central Asia. In: Robert M. Howard – Kirk A. Randazzo – Rebecca A. Reid (eds.): *Research Handbook on Law and Political Systems*. Cheltenham, Edward Elgar Publishing, 2023. 139-168.

[13] Б. А. Страшун: *Решения Конституционного Суда Российской Федерации как источник права. К 10-летию Конституционного Суда Российской Федерации. материалы международной конференции*. Москва, 2002. 162-172.

In 2017, a constitutional reform took place in Kazakhstan, which *"became a new logical stage on the path of a consistent comprehensive transformation of society and the state in line with the Kazakhstan-2050 Strategy"*, Kazakhstan's entry into the ranks of the thirty most developed countries. It crowns the implementation of five institutional reforms of the President of the Republic N.A. Nazarbayev and creates political and legal prerequisites for the qualitative growth of Kazakhstan within the framework of the third stage of modernization and ensuring the country's strong position in global competitiveness. The Republic of Kazakhstan is an example of the successful establishment of modern constitutionalism. The content of the Basic Law corresponds to the needs of the socio-economic, political, cultural, humanitarian and other spheres of life of every person, society and state, and the priority course of the country. Ensuring the inviolability of the foundations and implementing the latest achievements of constitutionalism, the effective combination of stability and dynamism of the Constitution, its responsiveness to the needs of social development are carried out through legislative and other implementation of the potential of the Constitution, as well as through timely introduction of changes and additions to the text of the Basic Law. This constitutional policy is under the leadership of the guarantor of the Constitution, the First President of the Republic – N.A. Nazarbayev and it is carried out systematically, on a deep scientific basis, with the most correct use of advanced foreign experience and the involvement of all segments of Kazakh society in the constitutional process.[14]

The constitutional reform of 2017 one of its objectives was the redistribution of powers between various government bodies. A number of innovations are aimed at ensuring the supremacy of the Constitution in the system of current law and its unconditional implementation throughout the country, improving government administration, strengthening the protection of constitutional rights and freedoms of human beings and citizens, and ensuring the fulfillment of constitutional duties by citizens.

In order to properly implement the novelties of the Law of March 10, 2017, the Head of State has set tasks to bring the entire body of the country's current law into conformity with the updated Constitution. In total, as a result of the work carried out by the Constitutional Council, 6 normative resolutions were reviewed and canceled in full and 21 – partially.

At the same time, those normative decrees that were not consistent with the amended and supplemented norms of the Basic Law were subject to abolition as a whole, and normative decrees were partially revised and repealed, with the

[14] Nora Webb Williams – Margaret Hanson: Captured Courts and Legitimized Autocrats. Transforming Kazakhstan's Constitutional Court. *Law & Social Inquiry*, 4/2022, 1201–1233.

exclusion of certain provisions that did not correspond to the constitutional innovations, the internal logic and interconnection were not lost, the content and meaning of the interpretation of the norms of the Constitution.[15]

In determining the procedure for executing the decision, the Constitutional Council indicated that the revision of normative resolutions does not mean the loss of legal force of the laws of Kazakhstan, as well as other legal acts related to these normative resolutions, or the return of legal force to acts previously recognized as unconstitutional. If necessary, these laws and relevant legal acts can be adopted, repealed, amended and supplemented in the prescribed manner.

The decision of the Constitutional Council opens up the scope for rethinking the content and nature of the noted and other constitutional provisions, which, if necessary, can be reinterpreted taking into account the results of the constitutional reform.

The Constitutional Council believed that legislative activity in the new conditions, as before, should be based on the rule of law, the most important components of which are legality, legal certainty, exclusion of arbitrariness, access to justice, respect for human and civil rights and freedoms, non-discrimination, justice and equality everyone before the law.[16]

5. Formation of the constitutional court in Kazakhstan

The nationwide referendum held in 2022 on amendments and additions to the Basic Law of the country – the Constitution of the Republic of Kazakhstan was a significant event for Kazakhstan. As a result of the referendum, 56 changes were made in accordance with the provisions of Article 33 of the Constitution. The purpose of the analysis of the changes made to the Constitution is to radically transition from the "super-presidential" governance model in the Constitution to a presidential republic with an influential Parliament and an accountable Government, to increase the influence of maslikhats, and to introduce a mixed majoritarian-proportional model of electing deputies of Majilis and regional maslikhats indicates that it is aimed at introduction. In addition, issues such as establishing the independence of the President from all political forces and parties, banning the close relatives of the Head of State from holding political positions and holding leadership positions in the quasi-state sector are also included. In addition, radical changes were made in the field of law enforcement. In particular, the Constitutional Court was established.

[15] Y. Abaydeldinov: Constitutional Court of the Republic of Kazakhstan. Continuity and innovation. *Bulletin of LN Gumilyov Eurasian National University Law Series*, 1/2023, 11–19.

[16] K. Bota: Constitutional policies of Kazakhstan. *European science review*, 3-4/2023, 19–33.

The status of the human rights representative, that is, the ombudsman, is established in the Constitution. The death penalty got completely abolished in our country. Among the changes and additions made to the Constitution, first of all, the issue of improving the model of constitutional control is of particular interest. According to the changes, the Constitutional Court started its activities from January 1, 2023. Now every citizen can directly protect his constitutional rights and freedoms in this body. Unlike the Constitutional Court and the Constitutional Council, citizens can apply directly to the new body. The Council did not consider such a possibility. Now the Constitutional Court examines the compliance of normative legal acts directly affecting their rights and freedoms with the Constitution at the request of citizens. In addition, the Prosecutor General and the Commissioner for Human Rights have the right to appeal to the Constitutional Court.

The institution of constitutional complaint is the most important means of protecting the rights and freedoms of a person and citizen, its implementation, according to scientists, "forms the basis of a modern democratic state".[17] N.S. Bondar considers the right of constitutional complaint to be *"an expression of the complex of constitutional rights, including not only the right to be protected by a court, but also the right to participate in the management of state affairs"*.[18] Increases the responsibility of the authorities to the people, as well as allows citizens, political parties and public associations to directly protect their violated rights at the highest constitutional level. Flora and fauna, other natural resources belong to the people. The value of this norm is to legally confirm that natural resources belong to the people, of course, it has a great impact on social and economic processes in society. Constitutional recognition of public property is an important historical step for the future development of Kazakhstan. It is the basis of an effective model that allows faster updating of economic legislation, and its goal should be to increase the standard of living and well-being of the citizens of Kazakhstan.

Another innovation in the Constitution of the Republic of Kazakhstan should be noted. Article 43 of the Constitution was supplemented with new paragraphs 3 and 4. According to them: the President of the Republic of Kazakhstan should not be in a political party during the exercise of his powers, and his close relatives do not have the right to hold the positions of state political servants, heads of quasi-state sector entities indicates a lack of views. For example, in the USA, South Korea, the Republic of Turkey and other presidential republics, heads of state retain their membership in a political party after being elected.

[17] М. М. Петина: Конститутционная жалоба в системе прав средств прав человека в России. 2023.

[18] Nikolay S. Bondar: Eternal constitutional ideals. How unchangeable are they in a changing world? *Gosudarstvo i pravo*, 6/2020, 20–34.

Previously, Azerbaijan had such a restriction on the President, who did not have the right to be a member of a political party during his entire presidential term. Currently, according to the Law "On Political Parties", Chairmen, deputy chairmen and judges of all courts of the Republic of Azerbaijan, Human Rights Commissioner of the Republic of Azerbaijan, military personnel, prosecutor's office, justice, internal affairs, national security, border service, customs, finance, tax authorities employees, etc. individuals cannot be members of political parties during the entire term of office. In other words, the law does not establish any imperative norm for the Head of State.[19]

In parliamentary countries such as Hungary, Israel, Germany, Italy, etc., however, there is no direct ban on leaving the party or suspending membership after being elected. It should be noted that this is practically impossible in foreign countries due to high political competition, mass media involvement in political life and other factors regarding the appointment of relatives of state leaders to high positions.

The President of the Republic of Kazakhstan is the highest official of the state. It is a guarantee of the rights and freedoms of a person and a citizen. Due to its special constitutional status and authority, it takes measures to protect the country's sovereignty, independence and state integrity of the territory, ensures the coordinated functioning and interaction of state authorities, and also determines the main directions of the state's internal and external policy.

In September 2022, additional amendments were made to the Constitution. On September 1, 2022, Head of State Tokaev announced the start of the election cycle in his Address to the People of Kazakhstan. On November 20 last year, extraordinary presidential elections were held in Kazakhstan in accordance with the updated Constitution. For the first time, the Head of State was elected for a seven-year term without the right to re-election. The single-term Presidential initiative is a logical continuation of the steps taken to finally move away from the super-presidential model. The one-time introduction of the presidential term thus closes the process of institutionalization of the presidential republic with an optimal balance of power. The basis of this initiative is, on the one hand, 7 years is a sufficient period to implement any large-scale program and fulfill promises to the people, to implement major projects for the country. On the other hand, the limitation of the presidential mandate to one term can ensure that the Head of State is more focused on solving the strategic tasks of national development.

[19] C. Qaracayev: Individual constitutional complaint in the Republic of Azerbaijan. *Науковий вісник Міжнар родного гуманітарного університету. Сер.: Юриспрур денція*, 63/2023, 34–37.

Another important direction of changes and additions to the Constitution is the increase in the influence of the Parliament. First of all, according to the new wording of Article 50, Clause 3 of the Constitution, a mixed election system with proportional and majoritarian methods was introduced during the creation of Majilis. 30 percent of Majilis deputies, and 50 percent of maslikhat deputies in regions and cities of republican significance are directly elected through one-mandate district. With the adoption of the 1995 Constitution adopted in the republican referendum in the Republic of Kazakhstan, the majoritarian election system was approved at all levels. In 2007, after the next constitutional reform, during the formation of the Majilis of the Parliament, there was a full transition to the proportional system of forming the lower house of the Parliament. Returning to the majoritarian-proportional system of forming the representative bodies of power increases the motivation of voters, their active participation and activates the election processes in the country. The electoral system is a political consideration that it is able to give a certain impetus to reconstructions, to improve the legislative process and public administration, the electoral legislation of Kazakhstan can accept the needs and demands of the society as much as possible.

6. Conclusion

Based on the above, the proposal of the head of state to move to a new model of formation and interaction of power institutions and transformation of political processes in society can pave the way for new development. Amendments to the Constitution are aimed at ensuring the constitutional security of the country, improving the legislation, strengthening the welfare of the people and increasing the standard of living of the citizens of Kazakhstan, in particular:

1. The Constitutional Court, being an important part of the system of checks and balances in any country, controls other branches of government and prevents them from adopting laws that violate the constitutional rights of citizens. The presence of such a court ensures more effective implementation of the provisions of the Basic Law.

2. The wealth of land, subsoil, flora and fauna, of course, belongs to the nation. In many countries, this rule exists in different formulations. On the other hand, it is difficult to imagine that every citizen manages the underground treasury himself – it will lead to chaos. Therefore, there is a state in the management system. The state is representative of the entire people, because the president is elected by the people, parliamentarians are elected by the people, and the government

is approved by the president's proposal. The state rules over the land and its subsoil on behalf of the people of Kazakhstan. Therefore, this change to the Constitution does not mean that every citizen of the country will receive direct income. However, the benefits of the earth's surface and wealth affect everyone. The ownership of the land of Kazakhstan by the people is an imperative norm and this is an imperative norm and the main part of the constitutional provision.

3. The norm of terminating the membership of the ruling party during the term of office of the president increases political competition, creates equal conditions for the development of all parties, promotes the emergence of new political parties and movements, and has a positive effect on the political situation in the country.

4. The introduction of a one-time presidential term without the right to re-election seems to be an important step towards softening the power of the president and giving more power and opportunities to the government and parliament. Political reforms and institutional restructuring are aimed at increasing the responsibility of the state and state bodies to citizens, promoting economic and social development.

5. In connection with the transition to a mixed electoral system in the Majilis of Parliament and maslikhats, the entire system of holding elections was reorganized. The Mazhilis of the Parliament will work according to the new system, some of the deputies will be elected according to party lists, and some will be elected according to single-mandate territorial constituencies. This means that a part of the deputies will be elected through party lists, and a part will be elected by the people directly.

The decision to introduce a mixed proportional-majoritarian system of elections creates a more harmonious election model that ensures the rights of citizens and lays the foundation for a new format of relations between the people and their elected representatives.

The implementation of these measures will be an indispensable condition for further consolidation of the ideas of the rule of law and constitutionalism in Kazakhstan, it will minimize constitutional risks and threats and ensure constitutional legitimacy in the state.

Bibliography

Y. Abaydeldinov: Constitutional Court of the Republic of Kazakhstan. Continuity and innovation. *Bulletin of LN Gumilyov Eurasian National University Law Series*, 1/2023, 11–19.

Zaure Ayupova: Constitutional Liberties in the Republic of Kazakhstan. *Tulsa Journal of Comparative and International Law*, 1/1998, 77–86.

Nikolay S. Bondar: Eternal constitutional ideals. How unchangeable are they in a changing world? *Gosudarstvo i pravo*, 6/2020, 20–34.

K. Bota: Constitutional policies of Kazakhstan. *European science review*, 3-4/2023, 19–33.

B. I. Ismailov: "The formation of a system of constitutional control in the law enforcement practice of foreign states." In: *All-Russian digital encyclopedia*. Portalus, Moscow, 2008.

Jakub Jakusik: Constitutional Reforms and the Circumstances Behind the Transition of Power in the Republic of Kazakhstan. In: Gulayhan Aqtay – Cem Erdem (eds.): *Language and Society in Kazakhstan. The Kazakh Context*. Poznań, Adam Mickiewicz University, 2020. 59-70.

C. Qaracayev: Individual constitutional complaint in the Republic of Azerbaijan. *Науковий вісник Міжнар родного гуманітарного університету. Сер.: Юриспрур денція*, 63/2023, 34–37.

Alexei Trochev – Alisher Juzgenbayev: Instrumentalization of constitutional law in Central Asia. In: Robert M. Howard – Kirk A. Randazzo – Rebecca A. Reid (eds.): *Research Handbook on Law and Political Systems*. Cheltenham, Edward Elgar Publishing, 2023. 139-168.

Nora Webb Williams – Margaret Hanson: Captured Courts and Legitimized Autocrats. Transforming Kazakhstan's Constitutional Court. *Law & Social Inquiry*, 4/2022, 1201–1233.

А. И. Зыбайло: Конституционный контроль и международные обязательства государств. In: *Вестник Института законодательства Республики Казахстан*. – № 4 (24). Almaty, 2011.

И. И. Рогово – В. А. Малиновского: *Конституционный контроль в Казахстане. Доктрина и практика утверждения конституционализма*. Almaty, 2015.

К. М Муканова: Становление и развитие института конститутционного контроля в РК. ББК 74.58 М 75, 182.

И. Ю. Остапович: *Конституцтционный Совет Республики Казахстан. Вопросы теории и практики*. Томск, 2005.

М. М. Петина: Конститутционная жалоба в системе прав средств прав человека в России. 2023.

И. И. Рогова – А. К. Котова: *Конституционный контроль в Казахстане*. Алматы, 2005.

Б. А. Страшун: *Решения Конституционного Суда Российской Федерации как источник права. К 10-летию Конституционного Суда Российской Федерации. материалы международной конференции*. Москва, 2002. 162-172.

VIOLATION OF THE RIGHT TO LIFE OF THE ROHINGYA REFUGEES

Md Razidur Rahaman[1]

ABSZTRAKT ■ Mianmar etnikailag sokszínű ország, ahol az 1982-es mianmari állampolgársági törvény alapján 140 csoport közül 135 elismert etnikai csoport található. Sajnos a muszlim többségű rohingya etnikai kisebbségi csoport (becslések szerint 2,5 millió ember, akik Mianmar Rakhine államában élnek) nem szerepelt az elismert csoportok között. Ennek eredményeként hontalanná váltak. Az ENSZ főtitkára, Antonio Guterres a rohingyákat „a világ egyik, ha nem a leginkább diszkriminált népcsoportjának" nevezte, akik nem részesülnek a legalapvetőbb jogok elismerésében, kezdve az állampolgársághoz való jog elismerésével saját országuk, Mianmar részéről. A főtitkár konfliktusok során fellépő szexuális erőszakkal foglalkozó különleges képviselője, Pramila Patten megjegyezte, hogy a rohingya nép a világ legüldözöttebb népe. Az ilyen üldöztetés következtében az élethez való elidegeníthetetlen joguk sérül, és különböző jelentések szerint rohingyák ezreit ölték meg a Mianmari Biztonsági Erők. Az élethez való jogot az Egyesült Nemzetek Szervezetének keretrendszerén belül különféle nemzetközi emberi jogi eszközök, valamint különböző regionális emberi jogi eszközök garantálják. Jelen tanulmány a rohingyák elleni rendszerszintű jogsértéseket tárgyalja, amelyek az élethez való jog megsértésére is kiterjednek..

ABSTRACT ■ Myanmar is an ethnically diverse country with 135 recognized ethnic groups among 140 groups under the 1982 Citizenship Law of Myanmar. Unfortunately, the Muslim majority Rohingya ethnic minority group, (estimated 2.5 million people, living in Rakhine State of Myanmar) was not among the recognized groups. As a result, they became stateless. The Secretary General of the United Nations Antonio Guterres described Rohingya as "one of, if not the, most discriminated people in the world, without any recognition of the most basic rights starting by the recognition of the right of citizenship by their own country Myanmar". The Special Representative of the Secretary-General on sexual violence in conflict, Ms. Pramila Patten, commented that the Rohingya people are the most persecuted people in the world. As a result of such persecution their inalienable right to life is violated and thousands of Rohingya have been killed by the Myanmar Security Forces, different reports show. Right to life is guaranteed under various international human right instruments under the United

[1] PhD Student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

Nations Framework as well as under different regional human rights instruments. This paper will discuss the systematic violations against Rohingya, which extend to the right to life.

Keywords: Rohingya, Refugee, Right to Life, jus cogens, Bangladesh, Myanmar, International Law

1. Introduction

Myanmar, a Southeast Asian country, is bordered by Tibet, China, Laos, Thailand, the Andaman Sea, the Bay of Bengal, Bangladesh, and India.[2] There are 54.7 Million people in Myanmar as of 2023.[3] Myanmar is predominantly Buddhist-dominant, with 89.8% of the population being Buddhists, with other religious groups including Christians, Muslims, Hindus, Animists, others, and people with no religion.[4] Myanmar is grappling with numerous socio-economic and political issues, including numerous armed and ethno-religious conflicts. Myanmar's history reveals freedom myths, particularly for minorities, with debates on independence focusing on internal tensions like the Rohingya Muslims-Rakhine Buddhists conflict in western Rakhine.[5] The Rohingya issue has become a global issue, not just a local one, due to the crimes committed against them. The Rohingya ethnic minority in Myanmar faces global issues, including transnational security, human rights violations and international claims, highlighting the need for global solutions.[6] This paper analyzes the systematic violations against Rohingya in Myanmar, including torture, death, and house burning, extending it to their right to life.

2. Research Methodology

The doctrinal research method is used in this research as research methodology. The doctrinal research is based on the review of the literature of primary and

2 Myanmar National Portal, https://myanmar.gov.mm/geography.

3 Myanmar Population 2023,https://worldpopulationreview.com/countries/myanmar-population.

4 The 2014 Myanmar Population and Housing Census, Census Report Volume 2-C, *The Union Report: Religion*. 2016/3,https://myanmar.unfpa.org/sites/default/files/pub-pdf/UNION_2C_Religion_EN.pdf.

5 MD Jobair Alam: The Rohingya Minority of Myanmar. Surveying Their Status and Protection in International Law. *International Journal on Minority and Group Rights*, 25(2)/2018, 157-158.

6 Ibid. at 159.

secondary sources and it is largely used as research methodology in this research. Doctrinal research is used in explaining the present international law framework to protect the right to life.

3. Background of the Rohingya Refugee Crisis

Myanmar has 135 recognized ethnic groups under the 1982 Citizenship Law, including the Rohingya, who have a history dating back hundreds of years, as noted by Dr. Francis Buchanan-Hamilton in 1799. Buchanan-Hamilton, a British physician and geographer, noted that the Mohammedans, who settled in Arakan, are known as 'Rooinga' while the Rakhine adhere to Buddha's teachings.[7] Arakan Arakan was independent from 1430 to 1784 until the Burmese King Bodawpaya conquered and dominated it until 1824.[8] Arakan Arakan, once independent, fell under British domination in 1826 after the Anglo-Burman War, resulting in a prolonged armed conflict along the Bengal-Arakan border.[9] During British rule, Buddhists were less supportive, leading to Muslims gaining administrative positions. During WW2, Japan invaded Burma, leading to conflicts between the Burmese and the Rohingya, with the Burmese receiving support from Japan and the Rohingya receiving support from Britain.[10] Burma gained independence in 1948, leading to increased political violence among ethnic minorities. The British Government failed to establish an independent Muslim state, but created a Mujahid movement demanding autonomy. In 1961, the U Nu government signed ceasefire agreements with Mujahid groups and established the Mayu Frontier Administration Area, covering Maungdaw, Buthidaung, and Western Rathedaung districts.[11] Under General Ne Win, the oppression of Rohingya intensified, with human rights abuses and forced labor becoming

7 Rubiat Saimum: No Place to Call Home: Historical Context, Statelessness and Contemporary Security Challenges of Rohingya Refugee Crisis. *BIMRAD Journal*, 3(1)/2022, 4.

8 Nasir Uddin: *The Rohingya: An Ethnography of 'Subhuman' Life*. November 2020, Oxford University Press.

9 Crimes against Humanity in Western Burma: The Situation of the Rohingyas, *Irish Centre for Human Rights*, 24/2010, https://burmacampaign.org.uk/images/uploads/ICHR_Rohingya_Report_2010.pdf.

10 History of the Rohingya, Rohingya Cultural Center Chicago, https://rccchicago.org/history-of-the-rohingya/.

11 MD Razidur Rahaman: Rohingya. The Community of No Human Rights. *The Daily Observer*, 2017, https://observerbd.com/details.php?id=68541.

routine in ethnic minority regions, particularly under the "Four Cuts" military operation.[12]

4. Persecution against Rohingya, which extends to Violation of the Right to Life

The Rohingya people faced violence in 1977 under General Ne Win's "Operation Nagamin" before returning after a treaty arrangement between Bangladesh and Myanmar. The Rohingya people, who were denied citizenship in Myanmar through the 1982 Citizenship Law, have been declared 'Stateless'. Section 2 of the 1982 Citizenship Law outlines three types of citizenship: Burma Citizens, Associate Citizens, and Naturalized Citizens. Burma citizens include nationals and ethnic groups settled in territories from 1185 B.E. to 1823 A.D[13] or, every national and every person born of parents, both of whom are nationals, are citizens by birth.[14] The Council of State can grant or revoke citizenship, associate or naturalized citizenship to any person, except those citizens by birth, in the State's interest.[15] The Central Body can determine associate citizens for applicants under the Union Citizenship Act of 1948, based on their qualifications and stipulations.[16] Individuals and their offspring(s) born before January 4th, 1948, who haven't yet applied under the Union Citizenship Act, 1948, can apply for naturalized citizenship through conclusive evidence.[17] To gain Myanmar citizenship, Rohingya people must prove they lived in Myanmar before the Anglo-Burmese War in 1823. Since the first Anglo-Myanmar War, Rohingya have been illegal immigrants. Between 1991-1992, around 270,000 Rohingya entered Bangladesh, many returning to Myanmar in 1996. In 2012, violence against Rohingya escalated, with Burmese President Thein Sein admitting the persecution.[18] The former Foreign Minister of Myanmar, U Ohn Gyaw stated in 1992 that there has never been a "Rohingya" race in Myanmar, as Muslim immigrants from neighboring countries illegally entered Naing-Ngan since 1824, without immigration papers.[19] Human Rights Watch satellite images

12 Ibid.
13 Section 3 of the 1982 Citizenship Law.
14 Section 5 of the 1982 Citizenship Law.
15 Section 8 of the 1982 Citizenship Law.
16 Section 23 of the 1982 Citizenship Law.
17 Section 42 of the 1982 Citizenship Law.
18 Burma's junta admits deadly attacks on Muslims, *The Guardian*, 2012, https://www.theguardian.com/world/2012/oct/28/burma-leader-admits-attacks-muslims.
19 Ibid.

reveal the devastating destruction of Kyaukpyu, a town on the west coast of the Philippines, resulting in the loss of 811 buildings and houseboats. Thein Sein's spokesperson reported incidents of villages and towns being burned down, with the death toll initially set at 112, but later revised to 67.[20] Human Rights Watch reports 633 buildings and 178 houseboats destroyed in the Rohingya-occupied area. Nobel laureate Aung San Suu Kyi's committee of MPs has called for swift legal action against those responsible for the recent killings and destruction.[21] In 2016, Myanmar's army crackdown on Rohingya Muslims may have resulted in over 1,000 deaths, according to senior UN officials, indicating a higher death toll than previously reported.[22] Myanmar's presidential spokesman, Zaw Htay, reported that less than 100 people were killed in a counterinsurgency operation against Rohingya militants who attacked police border posts in October 2016.[23] After this latest persecution, around one million Rohingya people left Rakhaine state of Myanmar and have taken shelter in different Camps in Cox's Bazar district of the neighbouring country Bangladesh.

5. The refugee status of Rohingya under International Refugee Law

The 1951 convention "is both a status and rights-based instrument and is underpinned by a number of fundamental principles, most notably non-discrimination, non-penalization and *non-refoulement*." The 1951 Convention on the Status of the Refugees defined the term Refugee as a person who flees to a foreign country or power to escape danger or persecution "owing to well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his nationality and is unable or, owing to such fear, is unwilling to avail himself of the protection of that country; or who not having a nationality and being outside the country of his former habitual residence as a result of such events, is unable or, owing to such fear, is unwilling to return to it." Another important procedure is the 'Subjective test' and 'Objective test'. The Rohingya must refer to the 'fear of persecution', which is called the subjective test and suggest the fear is well-founded, which called the objective test. Now the question will come

[20] Supra Note. 17.

[21] Ibid.

[22] More than 1,000 Rohingya is feared to have been killed in Myanmar crackdown, say UN officials, *The Guardian*, 2017, https://www.theguardian.com/world/2017/feb/09/more-than-1000-rohingya-feared-killed-in-myanmar-crackdown-say-un-officials.

[23] Ibid.

to mind whether the Rohingya are fulfilling any element of the 1951 Refugee Convention and whether they can justify the subjective and objective tests. If we analyse the reasons, why Rohingya fled from Myanmar to various countries, particularly to Bangladesh we can easily find out that the main reason is religion. The Rohingya are Muslims in majority by religion and they were tortured by Buddhist people and also persecuted by the security forces of Myanmar. The Myanmar Border Guard Police (BGP) is involved in torturing, killing Rohingya and looting their property. It's clear that the "well-founded fear" is present in the situation of Rohingya in Myanmar. From the historical analysis it is clear that the only reason for such torture is the religion of the Rohingya in Arakan State in Myanmar. There is no doubt that the Rohingya have lost their national status by the government because of their religious belief, which satisfies the elements of the definition of refugee under article 1 of the 1951 Convention on the Status of the Refugees. The Rohingya are living in Bangladesh under temporary protection.

6. Importance of the Right to Life under International Law

The right to life is a very broad term. It is defined under the international legal system, including the Universal Declaration of Human Rights (UDHR) 1948, The American Declaration of the Rights and Duties of Man 1948 and the European Convention of Human Rights (ECHR) 1953. These three international law instruments defined the term *right to life* at the very beginning of the end of the Second World War. The right to life, as described by the French League of Rights of Man before World War II, includes the right of mothers, children, women, old men, sick men and invalids to consider and care and supplies necessary for their social roles, physical and moral development and protection from exploitation.[24] The right to live includes limited work opportunities, fair compensation, access to scientific and technological progress, intellectual, artistic and technical development and care for those unable to work, ensuring equitable distribution and distribution of well-being.[25] Contemporary sources suggest that the right to life, as a legally enforced right, has modest dimensions. Article 6 of the International Covenant on Civil and Political Rights (ICCPR) states that every human has an inherent right to life and the death penalty is not imposed on minors or pregnant women. Article 2(1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950, asserts the

[24] Hugo Bedau: The Right to Life. *The Monist*, 52(4)/1968, 551.

[25] Georges Gurvitch: *The Bill of Social Rights*. New York, International Universities Press, 1946. 17-18.

same interpretation of the right to life as ICCPR stated in article 6. It stated that everyone's right to life is protected by law, except in court sentences for crimes provided by Article 6 of the International Covenant on Civil and Political Rights. During the Great Depression, historians cautiously noted that the right to life could be seen as an individual's emergency claim on society for sustenance.[26]

The Human Rights Committee on article 6 of ICCPR describes the right to life in its General Comment as the deprivation of life involves intentional harm or injury, including physical or mental harm.[27] Article 6 of the International Covenant on Civil and Political Rights protects the right to life for all human beings, even in armed conflict or emergencies. This fundamental right is crucial for individuals and the society, and its effective protection is necessary for the enjoyment of other human rights. It ensures individuals are free from unnatural or premature death and enjoy a life with dignity. The Inter-American Court of Human Rights ruled in *Villagran Morales V. Guatemala* that human rights encompass not only the right to life without arbitrary deprivation but also access to dignified living conditions.[28] The right to life is a distinct right involving liberty, self-development and self-perfecting. It is a fundamental aspect of other rights, as a deprivation of life results in loss of liberty, self-improvement and other rights, thus distinguishing it from other rights.[29] The right to life is often argued as an absolute, inviolable right, particularly by Roman Catholic moralists.[30] It is never lawful to terminate human life, and only in the hope of preserving or prolonging it can it be justified. The individual's life is sacred, and no human power can licitly kill an innocent person for any purpose. The State cannot put an unoffending man to death for its own existence.[31] The death-with-dignity movement aims to overturn the state's monopoly on lethal force and undermine the fundamental liberty idea of securing and protecting the right to life for everyone, regardless of their mental and physical capacity, by allowing assisted suicide and euthanasia.[32] Article 31 of the 1951 Convention on the Status of the Refugee protects the right to life of the refugees. The member States shall not

[26] Crane Brinton: Natural Rights. *Encyclopedia of Social Science,* 11/1933, 301.

[27] General comment No. 36, Human Rights Committee, September 2019, This general comment replaces general comments No. 6, adopted by the Committee at its sixteenth session (1982), and No. 14, adopted by the Committee at its twenty-third session (1984). Available at: CCPR/C/GC/36.

[28] Elizabeth Wicks: The Meaning of 'Life'. Dignity and the Right to Life in International Human Rights Treaties. *Human Rights Law Review,* 12(2)/2012, 202.

[29] H.J. McCloskey: The Right to Life. *Mind*, 84(335)/1975, 404.

[30] Ibid. at 422.

[31] McCloskey 1975, 422.

[32] Leon R. Kass: The Right to Life and Human Dignity. *The New Atlantis,* 16/2007, 24.

impose penalties on refugees from threatened territories who enter or remain in their territory without authorization, provided they present themselves and show good cause. Restrictions on refugees' movements are necessary until their status is regularized or they obtain admission into another country, with reasonable periods and necessary facilities.

7. The right to Life and Torture as *Jus Cogens* Norm in International Law

The right to life is a fundamental aspect of international law, enshrined in treaties, customs and *jus cogens*. Despite its importance, life remains cheap in many parts of the world, often due to excessive force or failure to investigate homicides.[33]Article 53 of the VCLT is enough to understand the importance of the *juscogens* norm. It stated that a peremptory norm is a norm of general international law that the international community of states of the United Nations has accepted and recognized as such. Approaching the right to life as a norm of *jus cogens*, the content of which is to be found in customary international law, reflecting the conscience of mankind, the great codified rights strengthen this most fundamental human right, For example, Article 3 of the Universal Declaration of Human Rights *stated that "Everyone has the right to life, liberty and security of person"*.article 6(1) of the International Covenant on Civil and Political Rights provides that, *"Every human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life"*, article 2(1) of the European Convention of Human Rights and Fundamental Freedoms stated that, *"Everyone's right to life shall be protected by law. No one shall be deprived of his life intentionally save in the execution of a sentence of a court following his conviction of a crime for which this penalty is provided by law",* and article 4(1) of the American Convention of Human Rights stated that, *"Every person has the right to have his life respected. This right shall be protected by law and, in general, from the moment of conception. No one shall be arbitrarily deprived of his life"*. A particularly significant illustration of the application of *jus cogens* can be seen in the Report on Human Rights in Chile, wherein the right to life was held to be a fundamental right in any society, irrespective of its degree of development or the type of culture'. Accordingly, the report concludes: The international community therefore considers the right to life in the context of *jus cogens* in international human rights law. It follows that its preservation is an essential function of the State, and numerous provisions of national legislation,

[33] Christof Heyns – Thomas Probert: Securing the Right to Life. A cornerstone of the human rights system. *EJIL Talk*, https://www.ejiltalk.org/securing-the-right-to-life-a-cornerstone-of-the-human-rights-system/.

including Chilean legislation, establish guarantees to ensure the protection of this right. The position defended by the contributors is that the right to life is an imperative norm, a peremptory right, that is, *jus cogens*. The ILC Draft Conclusion 4 of the Conclusions on Identification and Legal Consequences of Peremptory Norms of General International Law (*jus cogens*) stated that, a peremptory norm of general international law *(jus cogens)* is a norm accepted by the international community of States, allowing no derogation and only modifiable by a subsequent norm of the same character. The Conclusion 5 stated that, The International Law Commission (ILC) identifies customary international law as the most common basis for peremptory norms of general international law, with treaty provisions and general principles also potentially serving as bases. Precisely, the "right to life" is a norm of customary international law or a general principle of international law that transcends particular positions, as this right is codified in specific international conventions. Human rights lawyers are not restricted by specific conventions or declarations but must utilize all available evidence and practice within the international community. The further innovation becomes the scope, or the outer limits of the right to life. Nevertheless, two aspects of this right to life must be considered, as the contributors so aptly demonstrate. The physical existence of mankind must be guaranteed as a norm of *jus cogens*, which states cannot derogate, even during emergencies and warfare. Simultaneously, the "right to living" mandates maintaining a minimum quality of life. Governments have a legal duty to provide minimum subsistence levels. Obviously, the problem of setting such levels must, necessarily, be determined in each case, yet the significant consideration is that governments are required "to pursue policies which are designed to ensure access to the means of survival for every individual within its country." Related subject matter areas, such as the right to peace, the right to survival, and the right to a safe environment are applicable. Environmental hazards must not be minimized because the interrelationship between the right to live and the right to a pure and clean environment are inseparable. Not only is a strict duty imposed on states, but a legal obligation – a right *erga omnes* – is imposed on the international community. As a result, measures must be taken by international and regional organizations to prevent those environmental defaults that endanger the lives of human beings. Here, then, one of the newer human rights becomes an essential phase of the larger safeguard of human life. All too obviously, uncontrolled pollution has the potential not only of destroying flora and fauna but also mankind: it is humans who have become the endangered species.

The International Court of Justice ruled that any state's sovereignty-based reservation to the Genocide Convention is illegal, stating that genocide goes against moral law and UN aims. The International Court of Justice ruled that

the principles of the Convention are recognized by civilized nations as binding on States and that the contracting States have a common interest in achieving the high purposes of the Convention.[34] The International Court of Justice ruled in the Barcelona Traction case that states have obligations to the international community, including the prohibition of acts of aggression and genocide, as well as protection from slavery and racial discrimination. In 1973, Judge Fitzmaurice outlined "sundry current manifestations of naturalist-universalist thought and the principle of cooperation," including non-resort to force, non-recognition of situations involving force, and interdiction of crimes against peace and humanity.[35] Hersch Lauterpacht, Judge on the International Court of Justice, then Special Rapporteur to the International Law Commission, included in his 1953 Report on the Law of Treaties a draft article 15 reading: "A treaty, or any of its provisions, is void if its performance involves an act which is illegal under international law and if it is declared so to be by the International Court of Justice." The object's illegality and nullity are not due to a mere violation of customary international law but to inconsistencies with overriding principles of international public policy. Article 3 of the Universal Declaration of Human Rights (UDHR) aims to safeguard for everyone's inalienable right to life. However, the world has witnessed horrific human rights violations for a long time, including in 2013 and the latest persecution in the late 2016 and the first half of 2017 during the persecution against Rohingya in Myanmar. In 2013, The Myanmar Police fired and killed pregnant Rohingya Women.[36] Thousands of Rohingya have been killed, including women and children; people have been beaten and tortured; girls and women raped; houses and other properties burned.[37] Four Rohingya children, two of them were eight and two were ten years of age, were killed in a landmine explosion in Myanmar's western Rakhine state.[38] A Rohingya woman Noor Ayesha said that her five children were burnt to kill by the Myanmar Security Forces and they killed her two daughters after being raped in 2016 during persecution.[39] The UNICEF

[34] Marjorie M. Whiteman: *Jus cogens* in International Law, with a Projected List. *Georgia Journal of International and Comparative Law*, 7(2)/1977, 609.

[35] Ibid. at 611.

[36] Three Rohingya women killed in Burma shooting, 5 June 2013, *BBC News*, https://www.bbc.com/news/world-asia-22780085.

[37] S. K. Behera – G. S. Nag (eds.): *The Rohingya crisis mapping the conundrum and challenges of peace building: Selective South Asian perspectives*. Lulu Publication, 2021. 85-106.

[38] Kyaw Ye Lynn: Landmine kills 4 Rohingya children in Myanmar, 2020, https://www.aa.com.tr/en/asia-pacific/landmine-kills-4-rohingya-children-in-myanmar/1694946#.

[39] Burmese military killed seven of my children, says Rohingya refugee, *The Guardian*, 2016, https://www.theguardian.com/world/2016/dec/10/burmese-military-killed-seven-of-my-children-says-rohingya-refugee.

stated that 143 children were killed or wounded in numerous civil wars being fought along Myanmar's porous borders.[40] A survey conducted by Médecins Sans Frontières (MSF) in refugee settlement camps in Bangladesh estimated that at least 9,000 Rohingya were killed in the Rakhine state of Myanmar between 25 August and 24 September 2016 during the persecution by Myanmar Security Forces.[41] 71.7% of reported deaths were violence-related, resulting in at least 6,700 deaths, including 730 children under five.[42]

Therefore, article 6 of the Convention on the Rights of the Child (CRC) states that the state parties recognize that every child has the inherent right to life and they will ensure the survival and development of the child to the maximum extent possible. Myanmar ratified the CRC. As a member state of the CRC, Myanmar has responsibility to protect children's inherent right to life. But instead of protecting, they have killed thousands of children. Article 10 of the Convention on the Rights of Persons with Disabilities affirms the inherent right to life, emphasizing equal enjoyment for all individuals with disabilities. Article 4 of the African Charter on Human and Peoples' Rights asserts that all individuals are inviolable and entitled to respect for their life and integrity. Article 2 of the European Convention on Human Rights states that everyone's right to life shall be protected by law. Article 2 of the European Charter of Fundamental Rights states that everyone has right to life, even restricting the death penalty. The Human Rights Committee under ICCPR in its General Comment No. 36 states that, States have a duty to protect life by addressing social conditions, ensuring access to essential goods and services, raising awareness of gender-based violence, and improving access to medical examinations and treatments designed to reduce maternal and infant mortality. The right to life is a fundamental human right recognized worldwide as a necessary prerequisite for the enjoyment of all other human rights.[43] The Inter-American Court of Human Rights (IACHR) emphasized the human right to life, stating that every individual has an inalienable right to be respected and not arbitrarily deprived of it.[44] The right to a healthy environment and peace are seen

40 Shoon Naing: Four Rohingya children killed in blast in Myanmar's Rakhine state. *Reuters*, 2020, https://www.reuters.com/article/us-myanmar-rohingya-explosion-idUSKBN1Z61K1.

41 MSF surveys estimate that at least 6,700 Rohingya were killed during the attacks in Myanmar, MSF, 2017, https://www.msf.org/myanmarbangladesh-msf-surveys-estimate-least-6700-rohingya-were-killed-during-attacks-myanmar.

42 Ibid.

43 F. Przetacznik: The Right to Life as a Basic Human Right. *Revue des droits de l'homme/Human Rights Journal*, 9/1976, 589, 603.

44 IACHR, Advisory Opinion OC-3/83,, A/3. 1983. 53, 59.

as extensions or corollaries of the right to life.[45] The right to life, in its modern sense, protects against arbitrary life deprivation and mandates states to ensure survival through policies[46] for all individuals and all people. States are obligated to prevent severe environmental hazards or life-threatening risks by implementing monitoring and early-warning systems and urgent-action systems to detect and address such threats.[47] The First European Conference on the Environment and Human Rights (1979) emphasized the need for humankind to protect itself from environmental threats that negatively impact life, health, and future generations.[48] The right to life, in its broadest sense, necessitated the recognition of the right to a healthy environment.[49] The right to a healthy environment protects human life through its physical existence, health, dignity, and quality of life, making it worth living.[50] The right to life and a healthy environment is broadened by the characterization of threats against these rights, necessitating a higher level of protection.[51] The maintenance of peace is imperative for the preservation of human life which has been expressed in the UN Charter (preamble and Articles 1 and 2) and the UNESCO Constitution (preamble and Article I).

8. The accountability of Myanmar Under International Law

The UN was established after the mass destruction of human civilization after the Second World War. The object and purpose of establishing the UN is to promote and protect international peace and security in accordance with the Charter of the United Nations. Member states are committed to respecting international principles enunciated in the charter of the United Nations. Myanmar, as a member state of the UN, is bound to respect the principle of the UN Charter. But it is very unfortunate that Myanmar has not shown respect to protect human rights and peace within its territory for a long time. Continuously, the country is violating

45 B. G. Ramacharan: The Right to Life. *Netherlands International Law Review*, 30(3)/1983, 303, 308-310.

46 Ibid. at 302.

47 Supra Note. 31, at 304, 329.

48 P. Kromarek: Le droit à un environnementéquilibré et sain, considérécomme un droit de l'homme: sa mise-en-oeuvre rationale, européenne et internationale. Conférenceeuropéenne sur l'environnement et les droits de l'homme, 1979. 2-3, 31.

49 Ibid. at 13.

50 Ibid. at 12.

51 J.T.B.Tripp: The UNEP Montreal Protocol: Industrialized and Developing Countries Sharing the Responsibility for Protecting the Stratospheric Ozone Layer. *New York University Journal of International Law and Politics*, 20/1988, 734.

the human rights of Rohingya and the security forces and the Buddhist extremist groups are persecuting the Rohingya people. In the persecution of 2017, around one and a half million Rohingya crossed the border and took shelter in the neighboring country Bangladesh. Women were raped and tortured, men were also tortured. Bangladesh opened its border for the Rohingya to protect their human rights and to respect international law. The principle of *non-refoulement* has been recognized as a peremptory norm of international law and is therefore binding on the destination states despite the fact that they are not a member of the 1951 Convention relating to the Status of Refugees. The principle of *"Non-refoulement"* is a very protective principle for the refugees. It is considered as the most fundamental principle of international refugee law. *Non-refoulement* shall be considered as a peremptory norm when there is possibility of non-discrimination, genocide, use of force, crime against humanity or slavery. In the Rohingya issue, Bangladesh forcefully refouled the Rohingya to Myanmar and there is a high possibility of persecution or crime against humanity when this happened to the Rohingya by the Myanmar security forces or its citizens. The peremptory norm is an overriding principle, where no derogation is permitted. According to Elihu Lauterpacht and Daniel Bethlehem, "*Non-refoulement* is a concept which prohibits States from returning a refugee or asylum seeker to territories where there is a risk that his/her life or freedom would be threatened on account of race, religion, nationality, membership of a particular social group, or political opinion."[52] Article 33(1) of the 1951 UN Refugee Convention states that, "No Contracting State shall expel or return ("refouler") a refugee in any manner whatsoever to the frontiers of territories where his life or freedom would be threatened on account of his race, religion, nationality, membership of a particular social group or political opinion." *Non-refoulement* is a non-derrogable right of the refugees. It's ensured by the 1951 refugee Convention. Article 42(1) of the 1951 refugee convention specifically provides that the states cannot make reservation on article 33, which deals with the principle of *Non-refoulement.* Article III(5) of *the* Cartagena Declaration 1984 provided that the principle of *non-refoulement* as a "cornerstone of the international protection of refugees" and stated that *"this principle is imperative in regard to refugees and in the present state of international law should be acknowledged as jus cogens."* The General Conclusion (Conclusion No-25(xxxiii)-1982) of the Executive Committee on the International Protection

[52] Elihu Lauterpacht – Daniel Bethlehem: The Scope and Content of the Principle of Non-Refoulement. Opinion. In: Erika Feller – Volker Türk – Frances Nicholson (eds.): *Refugee Protection in International Law. UNHCR's Global Consultations on International Protection*. Cambridge University Press, 2003. 87-177. 89,http://www.refworld.org/docid/470a33af0.html.

of Refugees, 1982, *"reaffirmed the importance of the basic principles of international protection and in particular the principle of non-refoulement which was progressively acquiring the character of a peremptory rule of international law".*

Myanmar ratified the VCLT, 1969 in 1992. So, Myanmar has the obligation to respect articles 53 and 64 of this Convention. Myanmar is torturing and killing the Rohingya population inhumanely. Myanmar Security Forces set their houses on fire and forcefully deported them to the neighboring country, particularly to Bangladesh, which is the violation of the Rome Statute. According to the Rome Statute "Attack directed against any civilian population means a course of conduct involving the multiple commissions of acts against any civilian population, pursuant to or in furtherance of a State or organizational policy to commit such attack". The contextual element is that the 'acts' provided under article 1 of the Rome Statute will be considered as Crimes Against Humanity if the 'act' is committed as 'Widespread or Systematically', with the knowledge of the consequences of such attack (mental element), against any civilian population. The victim of 'Crimes Against Humanity' can be any resident regardless of their association or identity. In the situation of Rohingya in Myanmar, the Myanmar Military Ruler 'Systematically' denied citizenship from Rohingya in 1982 by adopting the "1982 Citizenship Act"; though they were citizens, even if they had been members of parliament as well, but since then they are "Stateless". The Citizenship Act excluded Rohingya as Nationals.[53] They have been forced to de-Islamize themselves, physical extermination through genocide and ethnic cleansing took place against the Rohingya.[54] The main intention of the military junta is to establish a Burmese Buddhist Arakan by destroying Rohingya Muslims in Arakan. The Security force, especially Nay-Sat-Kut-Kwey (NASAKA), of Myanmar is committing genocide against the Rohingya. NASAKA is formed by the Police, Military Intelligence, Lon Htein (internal security or Riot Police), Customs Officials, the Immigration and Manpower Department. The attack against Rohingya civilians was "systematic" and "widespread", which satisfied the requirement of crime against humanity under international criminal law.[55] In 1915, the allied governments of France, Great Britain and Russia used 'Crimes Against Humanity' to condemn Armenian mass killings in the Ottoman Empire. Following World War 2, it was prosecuted at the International Military Tribunal in Nuremberg. Since then, it has evolved under Customary International Law. The prohibition of crimes against humanity is a 'Peremptory Norm' of international

[53] Supra Note. at 10.

[54] Ibid.

[55] Crimes Against Humanity in Western Burma: The Situation of the Rohingyas, , *Burma Campaign UK*, http://burmacampaign.org.uk.

law, allowing no derogation and applicable to all states. Article 53 of the Vienna Convention on the Law of the Treaties, 1969, states that a treaty is void if it conflicts with a peremptory norm of general international law. For the purposes of this, a peremptory norm of general international law is a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character. Myanmar, which ratified the Convention in 1992, is violating these rules by torturing and killing the Rohingya population, setting their houses on fire and forcefully deporting them to neighboring countries, particularly Bangladesh. Arbitrary arrests, torture, custodial killings, rape, forced marriage, dishonouring of women, restriction on the socio-cultural and religious activities of the Rohingya are very common in Myanmar and as a consequence of this, millions of Rohingya left Arakan and have taken shelter in the neighboring country Bangladesh.

In March 2017, Yanghee Lee, the United Nations' Special Rapporteur for Human Rights in Myanmar, told the BBC that the government of Myanmar has to bear the responsibility for the "Systematic attack" against the Rohingya in Myanmar. She said, "I would say crimes against humanity. Definite Crimes Against Humanity by the Burmese, Myanmar military, the border guards or the police or security forces."[56] The United Nations conducted an interview with more than two hundred Rohingya who had fled from persecution in Myanmar, and prepared a report from the interviews. In this report the UN found that the security forces of Myanmar operated counter-military actions against Rohingya civilians and killed people, have brutally beaten them, raped women, and forcefully relocated them. On February 03, 2017, Former UN Human Rights Commissioner Zeid Ra'ad Al Hussein condemned the horrific cruelty done to Rohingya children, describing the mother's witnessing the murder of her child and the rape by security forces.[57] The OHCHR reported that the Security Force committed widespread human rights violations against Rohingya, which satisfied that the security force had committed crime against humanity.[58] On 6th February 2017, the former UN Special Adviser on the Prevention of Genocide, Adama Dieng, also said that the persecution of Rohingya could satisfy the elements of crime against humanity and that the scale of violence against Rohingya documented in the UN

[56] Aman Ullah: UN Commission of Inquiry for Myanmar, *The Stateless.com*, 2017, https://www.thestateless.com/2017/03/un-commission-of-inquiry-for-myanmar.html.

[57] "Devastating cruelty against Rohingya children, women and men detailed in UN human rights report", *OHCHR*, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21142.

[58] Ibid.

report represents a level of dehumanization and cruelty that is "revolting and unacceptable". It is expected from the United Nations to do justice to the Rohingya population and to take necessary actions to protect them.[59] UN Secretary-General Antonio Guterres mentioned the Rohingya as one of the world's most discriminated individuals, lacking basic rights, including citizenship recognition by Myanmar.[60] The Special Representative of the Secretary-General on sexual violence in conflict, Ms. Pramila Patten, commented that the Rohingya people are the most persecuted people in the world.[61] As a result of such persecution, their inalienable right to life is violated and thousand of Rohingya have been killed by the Myanmar Security Forces, different reports show. At least 34 of their houses got destroyed between January to March 2018 and 392 of their houses were burnt down and destroyed by the security forces between August 2017 and March 2018. Myanmar seized and bulldozed villages where Rohingya people lived and destroyed the proof of crimes they had committed and began to establish new bases for the security forces there.[62] Under the Contentious Jurisdiction, the ICJ discussed the case brought by Gambia on 11th November 2019 against Myanmar for violating its obligations under the Genocide Convention through acts against the Rohingya population.

The ICJ has jurisdiction to hear the case under article IX of the Genocide Convention as the States that are parties to Genocide Convention have no reservations to article IX. Article IX of this Convention stated that, the International Court of Justice will be consulted for disputes involving the interpretation, application, or fulfillment of the Convention, including state responsibility for genocide. Gambia basically urged the ICJ to take provisional measures against Myanmar and declare that it has committed Genocide against the Rohingya under article II of the Genocide Convention. It defines Genocide as any of the following acts committed with intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such: Killing members

[59] Violence in Myanmar's Rakhine state could amount to crimes against humanity, *The United Nations*, 2017, https://news.un.org/en/story/2017/02/550942-violence-myanmars-rakhine-state-could-amount-crimes-against-humanity-un-special.

[60] Transcript of Secretary-General's remarks at press encounter with President of the World Bank, Jim Yong Kim, 2018, https://www.un.org/sg/en/content/sg/press-encounter/2018-07-02/transcript-secretary-general%E2%80%99s-remarks-press-encounter.

[61] Human Rights Council opens a special session on the situation of human rights of the Rohingya and other minorities in Rakhine State in Myanmar, 2017, https://www.ohchr.org/en/press-releases/2017/12/human-rights-council-opens-special-session-situation-human-rights-rohingya.

[62] Roth Kenneth: Myanmar: Events of 2018, *Human Rights Watch*, 2019, https://www.hrw.org/world-report/2019/country-chapters/burma.

of the group; Causing serious bodily or mental harm to members of the group; Deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part; Imposing measures intended to prevent births within the group; Forcibly transferring children of the group to another group. In 2020, the Court found prima facie that a dispute existed between the Parties relating to the interpretation, application, or fulfillment of the Genocide Convention. Myanmar applied for time extension to submit a counter-memorial and the Court granted its extension to 24th August 2023. The trial should have been faster. Myanmar claimed that on August 25, 2017, ARSA militants attacked at least two dozen police posts and checkpoints and killed 11 members of the government Security Forces though the Rohingya community is denying such attacks. If we accept the claim of the Myanmar government that Rohingya 'terrorists' attacked the Security Forces of Myanmar, then how could Myanmar continue the brutal murders of Rohingya Muslims and set their houses on fire? If ARSA did such murders, Myanmar should have brought them under judicial trial and if they had been proven guilty, they would have been punished by the court of law. But what does Myanmar do instead of respecting and maintaining its National Legislation and respecting the International Human Rights Law as well as the principles of the charter of the UN is to protect international peace and security? The persecution of Rohingya by Myanmar Security Forces is not a new issue. It has been carried out since 1962 and until today it is going on. No one knows when, how or by whose leadership this persecution will be ended. Myanmar ratified the International Covenant on Economic, Social and Cultural Rights. The Rohingya populations do not get the basic right to education, which is a violation of article 13 and article 14 of this Covenant. Myanmar, as a member state of the prevention of discrimination on the basis of race, religion or belief; and protection of minorities, also has an obligation to ensure rights under this convention. Myanmar acceded to the convention on the elimination of all forms of discrimination against women. Myanmar also violated the principles contained in this convention by raping and torturing the women of the Rohingya community. The international community, especially the United States, China, Russia and the UK are silent about the genocide and crimes against humanity, which are going on against the Rohingya.

9. Conclusion

International law is developing, allowing states to admit refugees without fear of persecution, especially at their country's borders. However, admitting states may expel refugees, subject to treaty obligations, to another country.[63] The right to life is ensured under international human rights instruments. As human beings, the Rohingya people have their right to life, but in practice, Myanmar has deprived Rohingya people of the right to life for a long time. There are thousands of Rohingya who have been killed by Myanmar for a long time, but unfortunately, nothing happened to hold them accountable. It is time consuming to hold Myanmar accountable under international law, because the process of trying under international law is lengthy in nature. The issues may concern the International Court of Justice, which has the jurisdiction to deal with legal disputes submitted by states and provide advisory opinions on legal questions at the request of UN organs, specialized agencies, or related organizations, following international law. The ICJ provides advisory opinions on legal matters at the request of United Nations organs, specialized agencies, or related organizations authorized to make such requests. For this instance, the International Court of Justice has already taken the initiative in the Rohingya Genocide Case filed by Gambia. Bangladesh has taken some initiatives to return Rohingya refugees to Myanmar with the help of the UNHCR, but no positive progress has been seen. Without ensuring the safe place it is prohibited to return refugees to another country. Article 14 of the Convention Concerning Migration for Employment (Revised 1949) and the Model Agreement on Temporary and Permanent Migration for Employment prohibit the compulsory return of refugees to their country of origin. The United Nations General Assembly's Resolution (Resolution 8(I) of February 12, 1946, states that no refugees or displaced persons should be forced to return to their country of origin if their life or freedom is threatened for political, religious, or racial reasons. Myanmar also committed crimes against humanity to Rohingyas as it is very clear and satisfies the elements of crimes against humanity under article 7 of the Rome Statute. It stated that, Crime against humanity refers to acts committed in a systematic attack on civilian populations, including murder, extermination, enslavement, deportation, imprisonment, torture, sexual violence, persecution, enforced disappearance, apartheid, and other inhumane acts. The term 'attack directed against any civilian population' refers to a course of conduct involving multiple acts against civilians, aimed at committing such attacks, and

[63] Paul Weiss: The International Protection of Refugees. *The American Journal of International Law*, 48(2)/1954, 199.

is a violation of international law. Therefore, Rohingya refugees are living in different refugee camps in Cox's Bazar in Bangladesh. The living conditions are not good. There are shortages of food and medical care, which must be ensured for the lives of every person. Unfortunately, the donations are insufficient to accommodate this large number of vulnerable people and to provide their basic necessities. They don't have educational rights in Bangladesh, but they can access primary education in the Rohingya dialect within the camps with the help of different NGOs and with the support of the UNHCR. In exceptional cases, some Rohingya students get access to higher education in Bangladesh under the direct supervision of the UNHCR. They are engaging in smuggling and different crimes within the territory of Bangladesh. It creates security problems for Bangladesh. When they are engaged in crimes, they become more vulnerable. Moreover, there is no hope for a permanent solution in the near future. Their basic human rights are under shadow. No one cares about their right to life.

Bibliography

Aman Ullah: UN Commission of Inquiry for Myanmar, *The Stateless.com*, 2017, https://www.thestateless.com/2017/03/un-commission-of-inquiry-for-myanmar.html.

MD Jobair Alam: The Rohingya Minority of Myanmar. Surveying Their Status and Protection in International Law. *International Journal on Minority and Group Rights*, 25(2)/2018.

S. K. Behera – G. S. Nag (eds.): *The Rohingya crisis mapping the conundrum and challenges of peace building: Selective South Asian perspectives*. Lulu Publication, 2021. 85-106.

Hugo Bedau: The Right to Life. *The Monist*, 52(4)/1968.

Crane Brinton: Natural Rights. *Encyclopedia of Social Science*, 11/1933.

Elizabeth Wicks: The Meaning of 'Life'. Dignity and the Right to Life in International Human Rights Treaties. *Human Rights Law Review*, 12(2)/2012.

Georges Gurvitch: *The Bill of Social Rights*. New York, International Universities Press, 1946.

H.J. McCloskey: The Right to Life. *Mind*, 84(335)/1975.

Christof Heyns – Thomas Probert: Securing the Right to Life. A cornerstone of the human rights system. *EJIL Talk*, https://www.ejiltalk.org/securing-the-right-to-life-a-cornerstone-of-the-human-rights-system/.

Leon R. Kass: The Right to Life and Human Dignity. *The New Atlantis*, 16/2007.

F. Przetacznik: The Right to Life as a Basic Human Right. *Revue des droits de l'homme/Human Rights Journal*, 9/1976.

P. Kromarek: Le droit à un environnementéquilibré et sain, considérécomme un droit de l'homme: sa mise-en-oeuvre rationale, européenne et internationale. Conférenceeuropéenne sur l'environnement et les droits de l'homme, 1979.

B. G. Ramacharan: The Right to Life. *Netherlands International Law Review*, 30(3)/1983.

MD Razidur Rahaman: Rohingya. The Community of No Human Rights. *The Daily Observer*, 2017, https://observerbd.com/details.php?id=68541.

Rubiat Saimum: No Place to Call Home: Historical Context, Statelessness and Contemporary Security Challenges of Rohingya Refugee Crisis. *BIMRAD Journal*, 3(1)/2022.

Elihu Lauterpacht – Daniel Bethlehem: The Scope and Content of the Principle of Non-Refoulement. Opinion. In: Erika Feller – Volker Türk – Frances Nicholson (eds.): *Refugee Protection in International Law. UNHCR's Global Consultations on International Protection*. Cambridge University Press, 2003. 87-177. 89,http://www.refworld.org/docid/470a33af0.html.

J.T.B.Tripp: The UNEP Montreal Protocol: Industrialized and Developing Countries Sharing the Responsibility for Protecting the Stratospheric Ozone Layer. *New York University Journal of International Law and Politics*, 20/1988.

Nasir Uddin: *The Rohingya: An Ethnography of 'Subhuman' Life*. November 2020, Oxford University Press.

Marjorie M. Whiteman: *Jus cogens* in International Law, with a Projected List. *Georgia Journal of International and Comparative Law*, 7(2)/1977.

Paul Weiss: The International Protection of Refugees. *The American Journal of International Law*, 48(2)/1954.

THE EXTRATERRITORIAL EFFECTS OF DATA PROTECTION LAWS

Ali Sanar Shareef[1]

ABSZTRAKT ■ A joghatóság kérdésében, különösen az adatvédelemre tekintettel nincsenek egységes nemzetközi szabályok. A Lotus-ügyet számos állam precedensnek tekinti arra vonatkozóan, hogy a törvények alkalmazását a határain túlra is kiterjesztik. Mivel a digitális kor példátlan kihívásokat állít a fizikai határok elé, az államok között uralkodó tendencia, hogy elfogadják az ilyen törvények határokon átnyúló alkalmazását. Releváns nemzetközi jogszabályok hiányában azonban egyes államok extraterritoriális hatályt előíró adatvédelmi törvényeket fogadtak el, és nem korlátozták azok alkalmazási körét például a minimális kapcsolódásra vagy a fórumok alanyainak célzott szándékára. Ez ezen jogszabályok ütközéséhez, valamint a vállalatok és a weboldalak számára bizonytalansághoz vezethet. E tanulmány megvizsgálja, hogy az egységes nemzetközi jog hiánya miként vezetett az államok által elfogadott különböző megközelítésekhez, és az adatvédelmi törvények hatályának a határaikon kívülre történő kiterjesztéséhez, valamint elemzi ezen szabályozás lehetséges jogi következményeit. A tanulmány végül ajánlásokat fogalmaz meg a probléma kezelésére szolgáló mechanizmusokra, beleértve az egységes univerzális szabályok létrehozását.

ABSTRACT ■ data protection. The Lotus case is considered a precedent by many countries to extend the application of their laws beyond their borders. With the digital age presenting unprecedented challenges to physical borders, there is a prevailing trend among states to accept the cross-border application of such laws. However, in the absence of relevant international law rules, some states have enacted data laws with extraterritorial effects and without limitations on their scope, such as minimum connection or the intention to target forums' subject. This can lead to conflict of these laws and uncertainty for companies and websites. This study will examine how the absence of unified international law led to different approaches adopted by states in extending the reach of their data laws outside their borders, and the possibility of legal implications of these regulations. Finally, recommendations will be made for mechanisms to address the issue, including the establishment of unified universal rules.

Keywords: data protection, jurisdiction, extraterritorial effect, sovereignty

[1] PhD Student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

1. Introduction

Nothing has complicated legal jurisdiction more than the internet, marking the first time that jurisdiction has had to deal with individuals committing violations in the forum of other states, without being physically present. As the internet develops, so does online international business and vice versa[2]. Consequently, the increase in international transactions via internet poses greater challenges to the international legal system and states sovereignty. Due to its nature, internet contents cross borders and trigger multiple jurisdictions, and it becomes clear that mere domestic solutions are inadequate in addressing these challenges. Therefore, the development of international solutions for jurisdiction becomes inevitable[3].

The issue of jurisdiction in data protection presents a significant challenge due to the absence of a unified international legal framework governing jurisdiction. Consequently, it paved the way to governments to seek greater power internationally, aiming at extending their jurisdiction to cover as many cases as possible. While the protection of data is undeniably crucial, being both a human right and part of state security, it should not come at the expense of violating other international law principles, such as sovereignty, which is guaranteed by the UN Charter. The questions of jurisdiction are often intertwined with issues of state's sovereignty, territorial integrity, and non-intervention policies. Jurisdiction in the context of data protection law ought to be evaluated through the lens of public international law[4]. However, this rule is not absolute, there is an understanding among states to have at least a certain degree of extraterritoriality, but this is not open without limitations, rather there should be certain limitations. So having these laws now in itself is not a problem as the nature of internet and data compels that, but the problem lies in having these laws without any limitations on their scope, which can lead to, inter alia, conflict of law. The inherent nature of data in the digital era necessitates the existence of laws with cross-border reach, this

[2] In Hanson v. Denckla, the Supreme Court of U.S noted that *"[a]s technological progress has increased the flow of commerce between States, the need for jurisdiction has undergone a similar increase."* Twenty seven years later, the Court observed that jurisdiction could not be avoided *"merely because the defendant did not physically enter the forum state"*. The Court observed that: *"[I]t is an inescapable fact of modern commercial life that a substantial amount of commercial business is transacted solely by mail and wire communications across state lines, thus obviating the need for physical presence within a State in which business is conducted"*. Burger King, 471 U.S. at 476, 105 S. Ct. at 2184 https://law.justia.com/cases/federal/district-courts/FSupp/952/1119/1432344/ Accessed by 5/2/2024.

[3] R. Vaishnavi: Internet and Jurisdiction. Global Status. *Indian Journal of Law and Legal Research*, 5/2023, 1–9. 1.

[4] Stephan Kolossa: The GDPR's Extra-Territorial Scope. *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 4/2020, 791–818. 779.

in itself is not the problem. However, the problem arises when these laws are without clear limitations on their scope.

The complexities and sensitivities surrounding the matter are not adequately addressed or accommodated in the status quo[5]. Currently, many states have enacted data protection laws with extraterritorial effects. This situation has resulted in a proliferation of multi regulatory approaches, conflicts of law, and uncertainty for companies. The questions that arise here are: what is the concept of jurisdiction, especially when it comes to data protection? How does international law deal with jurisdiction in data protection? What is the international law perspective on laws with extraterritorial effects? How do different legislators tackle jurisdictional matters in data protection?

The study aims to explain how states extend their jurisdiction to reach entities located in other jurisdictions, focusing on the nuances of this extension's absoluteness and the lack of limitations on their scope, and recommending possible solutions.

The study is of great significance as it touches upon a universal issue bereft of universal rules, highlighting how the absence of international legal framework has led to the proliferation of laws with extraterritorial effects. It underscores the paramount challenges to data protection, especially in trans-border scenarios where multiple courts may claim jurisdiction in a single case.

For this purpose, we divided the study into five parts. The first part addresses the concept of jurisdiction. The second discusses the international legal framework for jurisdiction in data protection. The third delves into several examples of laws from different countries that exhibit extraterritorial effects. The final part analyses the Disparity in Degrees of Extraterritoriality in Data Protection Laws. Lastly, we will outline the recommendations and necessary steps that should be taken.

2. The concept of Jurisdiction

Jurisdiction is essentially the legitimate authority a state possesses to act in each matter[6]. This power, granted or confirmed by international law, enables it to conduct business, making decisions solving disputes[7]. The ability a state has to affect its legal concern is widely accepted as a foundational principle,

5 Vaishnavi 2023, 3.

6 Vaishnavi 2023, 2.

7 Joanna Kulesza: Transboundary Challenges to Privacy Protection in Cloud Computing. *Ukrainian Journal of International Law*, 2/2017, 117–128. 123.

which is commonly encapsulated in the term "jurisdiction"[8]. Unfortunately, the concept of jurisdiction is complex and not straightforward. We can say that it is a state's power to rule sovereignly by creating and exercising laws. In this sense, jurisdiction encompasses the commanding acts of all the three authorities of the state: legislative, executive, and judicial. In other words, jurisdiction reflects a state's sovereignty in relation to its three authorities[9].

Traditionally, jurisdiction consists of three types[10]: firstly, legislative (prescriptive, substantive), it is the state's power to implement its laws to cases that involve foreign elements. Secondly, judicial or adjudicative, which means the authority of the state's court to try cases include foreign component. Finally, executive one, which refers to the power of the state to perform actions in another state's territory[11].

The issue of jurisdiction, and whether national law applies to situations with links to several countries is not specific to data protection, or to the Internet. It is a general question of international law, which arises in on-line and off-line situations where one or more elements are present that concern more than one country. A decision is required on what national law is to be applied before a solution on substance can be developed.[12]

The problems of choice of jurisdiction, choice of applicable law and recognition of foreign judgements have proved to be complex in the context of trans border data flows. The question arose, however, whether and to what extent should it be attempted at this stage to put forward solutions in Guidelines of a non-binding nature[13].

The conventional approach to jurisdiction extends based on pecuniary, subject matter and territorial jurisdiction. However, in so far as the internet is concerned, there exist no physical, territorial boundaries, thus making the application of

[8] Kai Burmeister: Jurisdiction, Choice of Law, Copyright, and the Internet. Protection against Framing in an International Setting. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 2/1999, 625–723. 637.

[9] Krzystof Zalucki: Extraterritorial Jurisdiction in International Law. *International Community Law Review*, 4-5/2015, 403–412. 407.

[10] Amnesty International, Universal Jurisdiction. 4. https://www.amnesty.org/en/wp-content/uploads/2021/06/ior530032001en.pdf (accessed October 12, 2023).

[11] Christopher Kuner: Data protection law and international jurisdiction on the Internet (part 1). *International Journal of Law and Information Technology*, 2 /2010, 176–193. 184.

[12] Article 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites. Brussels, 2/2002. 2.

[13] OECD, Recommendation of the Council on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. https://www.oecd.org/digital/privacy/ : https://www.oecd.org/digital/privacy/, 46.

law extremely difficult. This becomes further challenging when a certain issue is legal in a country, but not in another country where the issue extends.[14]

2.1. Basis for jurisdiction

Public international law recognizes; when establishing a state's jurisdiction over persons, events, or goods; five basic principles, namely territoriality, effectiveness, personality, protection, and universality[15]. Domestic courts cite one or more of these principles to establish extraterritorial jurisdiction over crimes under national law of international concern as well as offences of international concern[16].

Territoriality: for a state to claim jurisdiction over a particular case, it must show evidence that the offense has taken place, in part or in whole, within its borders. This formulation was echoed in the lotus case and adopted by criminal codes of numerous countries.[17] Traditionally, jurisdiction over a person depends on their physical presence in the forum. However, the evolution of business life, especially the advancement of modem means of transportation and communication technologies, as well as commercial transactions involving parties in the entire country, challenged the traditional standards and requirements of the physical forum presence. As a result, courts began to exercise jurisdiction over persons who were not physically present in the court's forum, leading to the development of the minimum contact principle[18].

One of the state's main functions ensuring order within its territory[19], to this end the territoriality doctrine allows a state to govern the acts and behaviors of persons located within its boundaries. This doctrine plays a crucial role in the realm of data protection law. For example, article 4 (1)(c) of the EU data protection directive seems to reflect the principle of objective territoriality, as it is based on the occurrence of an act, or in other words the utilization of equipment within the EU[20].

Effects doctrine: the American law institute's restatement (second) of conflict of laws 37 (1971) defines the effect doctrine as the authority possessed by the state to assert judicial jurisdiction over a person for actions conducted elsewhere,

14 Vaishnavi 2023, 2.
15 Kulesza 2017, 123.
16 Amnesty International 2023, 9, 2.
17 Michael Akehurst: Jurisdiction in International Law. *British Year Book of International Law,* 46/1972-1973, 146–257. 152.
18 Burmeister 1999, 640.
19 Akehurst 1972, 152.
20 Kuner 2010, 188.

have consequences within it, provided these consequences give rise to a cause of action. Unless the nature of the effects and of the individual's connection to the state do not render the exercise of such power unreasonable[21].

Often, jurisdiction based on objective territorial principles, invoked via the effects doctrine, addresses acts that have caused or are aimed at causing harmful outcomes within a country's border. It is submitted that adopting 'primary effects' approach is more effective than 'constituent elements' in terms of maintaining state's jurisdiction within reasonable bounds[22].

Personality**:** there are three types of personality jurisdictions: the active one which relies on the nationality of the suspect, by contrast the passive one which considers the nationality of victim, the final one is protective, invoked when national interests are at risk[23]. The APEC Privacy Framework ensures the protection of personal data within APEC member states by emphasizing 'accountability'. According to this principle, the original data collector remains responsible for upholding privacy standards, even when data is transferred universally. This indicates that the privacy laws of the country from whom the data was collected continue to apply, regardless of the data's destination, that is to guarantee a continual protection[24].

Universality: this principle allows a court in any country to prosecute persons for crimes committed in another country, even if there is no link to the forum country through the nationality of the suspect or victim, or any harm to its own national interests[25].

Universal jurisdiction is still a developing concept within international law, lacking well-defined and established standards. The principle most closely allied to universal jurisdiction is *aut dedere aut judicare*. It obligates countries to either extradite or prosecute offenders found within their bounds. This term has often been used interchangeably with universal jurisdiction by scholars. Many international treaties and conventions included this principle in its provisions[26].

Some scholars and courts have posited that there is another form of extraterritoriality jurisdiction: the representational principle (which is based on the jurisdiction conferred upon a state by another state). However, when there

21 Betsy Rosenblatt: Principles of Jurisdiction. *Berkman Klein Center for Internet & Society at Harvard University*. https://cyber.harvard.edu/property99/domain/Betsy.html.

22 Akehurst 1972, 155.

23 Amnesty International 2023, Ibid.

24 Kuner 2010, 189.

25 Amnesty International 2023, Ibid.

26 Meghna Rajadhyaksha: Universal Jurisdiction in International Law. *Law Review, Government Law College* 2/2002-2003, 1–34. 2.

is no link to the exercising jurisdiction, this principle is simply an extension of universal jurisdiction[27].

2.2. Jurisdiction and internet

The question of state jurisdiction over personal data and individual privacy interests is demanding, the borderline of public and private law, making the, in itself ambiguous, distinction fairly irrelevant[28].

While enforcing national privacy and security laws falls within a state's jurisdiction and upholds its fundamental rights,[29] this authority isn't limitless. International law dictates that while states can legislate based on their interests, they must respect the legitimate interests of other nations.[30] As the Article 29 Working Party[31] acknowledges, data protection law jurisdiction is assessed through international law, due to the internet's global nature,[32] the general principles of international jurisdiction, present in international public law may be addressed to assert jurisdiction over personal data or protection of individual privacy[33]. Therefore, states aren't entirely free to establish unilateral rules. Instead, "reasonableness" governs their reach. As stated in section 421 of the Restatement (Third) of Foreign Relations, a state can exert court jurisdiction over a person or entity only if its connection justifies such an action. This implies balancing national interests with international legal principles and respecting other states' sovereignty[34].

3. International legal framework for Jurisdiction in data protection

The international framework governing jurisdictional issues in data protection is deemed insufficient, and there is no unified, legally binding international

27 Amnesty International 2023, Ibid.
28 Kulesza 2017, 123.
29 Ibid.
30 Burmeister 1999, 637.
31 The Article 29 Working Party (Art. 29 WP), established by Directive 95/46/EC, addressed privacy and personal data protection matters until May 25, 2018, when the General Data Protection Regulation (GDPR) came into effect, and its responsibilities were taken over by the European Data Protection Board (EDPB).
32 Kuner 2010, 184.
33 Kulesza 2017, 123.
34 Burmeister 1999, 639.

framework determining which state has jurisdiction over a specific case. All that we have are either non-binding guidelines or regional rules with limited application. There is no instrument under public international law of universal application containing jurisdictional rules for data protection law[35].

Back in 1999, the Hague Conference on Private International Law examined jurisdiction and applicable law in data protection during 'Geneva Round Table on Electronic Commerce and Private International Law'. However, this discussion didn't give any solution, except by issuing a statement that further investigation is needed[36].

Despite the recent attempts, the "Hague Conference" failed to make progress on a draft convention regarding the applicable law in contracts due to disagreements on the decisive criterion. This impasse indicates the heart of the problem: striking a fair balance between the diverse legal interests of involved parties.[37]

In 1999, the Hague conference on private international law jointly with Geneva university held The Geneva Round Table to explore the challenges facing private international law in the context of electronic commerce and the internet. The event spanned three days and convened in Geneva, Switzerland[38].

Back in 2005, the APEC Privacy Framework set guidelines for data privacy. Accordingly, each APEC economy should establish a legal framework that follows these principles. The framework ensures transferred data within the APEC region remains protected through the accountability principles.[39] But it contains no rule regarding jurisdiction in data protection.

In preparation for submitting it to the United Nations and under the chairmanship of the Spanish Data Protection Authority, a group of data protection authorities worldwide initiated the drafting of a universal legal instrument on data protection in 2009. Initial drafts included the following provisions that determined Jurisdiction over personal data processing based on the location of the responsible entity's operations or its targeted activities, with "establishment" broadly defined encompassing any stable operational presence. However, this provision was dropped in the final version[40].

35 Kuner 2010, 186.

36 Geneva Round Table on the Questions of Private International Law raised by Electronic Commerce and the Internet, organised jointly by the University of Geneva and the Hague Conference on Private International Law. Geneva, 2-4 September 1999.

37 Article 29 Data Protection Working Party, 5.

38 Stephen Kobrin: Safe Harbours Are Hard to Find. The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance. *Review of International Studies*, 1/2004, 111–131. 113. http://www.jstor.org/stable/20097901.

39 Ibid. 114.

40 Kuner 2010, 187.

Regulation (EU) No 1215/2012, enacted on 12 December 2012, set out rules governing jurisdiction and the recognition/enforcement of court decisions in civil and commercial matters across the European Union. Article 16 is designed to prevent individuals from facing unexpected lawsuits in foreign courts regarding privacy breaches or defamation, guaranteeing legal actions are predictable and just[41].

The Internet and Jurisdiction Global Status Report (2019) examines challenges posed by the cross-border nature of the internet, especially regarding jurisdiction issues and the rise in online crimes, heightened by the shift to online activities due to COVID-19. The report emphasizes the limitations of domestic approaches and the necessity for global frameworks due to conflicting legal priorities among countries. It stresses the need for a collaborative approach to address jurisdiction complexities, legal ambiguities, and potential negative impacts on global governance arising from inconsistent policies.

Given the above-mentioned issues, the report underscores the need to adopt a multistakeholder-based approach that is to begin at the earliest. It is crucial to investigate the seriousness of the issue domestically and adequately address the problems stemming from fragmented frameworks[42].

The Explanatory Memoranda of the OECD Privacy Guidelines highlights the problems of determining jurisdiction, applicable law and recognition of foreign judgements in the context of trans-border data flows. It raises the question of whether and to what extent it is appropriate at this stage to put forward solutions in Guidelines that are advisory and not mandatory[43].

The issues revolving around the internet and jurisdiction are still evolving in nature[44]. Political concepts of jurisdiction and community are not naturally defined, but socially constructed. In a world where spill-over and inter-jurisdictional conflict are becoming the norm and political space as a bounded geographic construct is losing meaning, establishing effective governance structures, which retain some sense of democratic legitimacy, may require reconceptualising both jurisdiction and political community[45].

41 Regulation (EU) No. 1215/2012 of the European Parliament and of the Council, of 12 December 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

42 The Internet and Jurisdiction Policy Network released their first-ever Global Status Report in Berlin on 27 November 2019.

43 OECD, Digital Economy Papers. No. 360, "Explanatory Memoranda of the OECD Privacy Guidelines". 2023. 22.

44 Vaishnavi 2023, 4.

45 Kobrin 2004, 113.

Sitting aside the complexity of jurisdiction, which is a complicated problem across all fields of law, data protection itself lacks worldwide rules governing its principles. The privacy rules that exist in human rights conventions are not sufficient to tackle data protection challenges, especially with the rapid increase of trans border commercial transactions. This is because the internet has made data protection issues more universal. Moreover, data protection issues extend beyond commercial concerns; they are surrounded by security dimensions on one side and political dimensions on the other. The security dimension relates to the transfer of subjects' data outside the country, which may pose threats to the national security of a state. States may try to expand their jurisdiction to have access to specific data, even abroad. On the other hand, governments attempt to enact domestic laws to access people's data within their country under the pretext of protecting national security. Sometimes political regimes use these laws for wiretapping opposition and activist calls. Therefore, predicting a breakthrough in the near future regarding the agreement on unified international rules is not feasible.

4. States' practice

When examining states' practice, it is clear that states frequently use a variety of standards to broadly define the boundaries of their domestic legal systems, to control conduct occurring outside of their boundaries, particularly concerning online activity[46].

The goal of providing broad protection to industry and national consumers is what motivates this strategy. As a result, circumstances involving cross-border components usually result in the application of several national laws[47].

Because so many governments are passing rules that apply to overseas businesses, the question of whether data laws have an extraterritorial reach has received a lot of attention. US officials contend that the effects of European data privacy regulations extend across national borders.[48] Article 29, on the other hand, asserts that in nations such as the United States, international websites are governed by national laws and municipal regulations because of domestic court decisions. The aforementioned conversation highlights the complex and interconnected terrain of global data governance, wherein nations wrestle with and establish control over data-related issues that transcend national

[46] Kuner 2010, 176.
[47] Article 29 Data Protection Working Party, 5.
[48] Kuner 2010, 176.

boundaries.[49] This debate has not emerged from nowhere, many states have laws with extraterritorial effects, leading to Legal complexity, uncertainty, and jurisdictional challenges. As demonstrated by examples such as Microsoft v. USA[50].

"Extraterritorial laws are laws in a given territory that can produce effects and be applicable within a sovereign foreign territory. A major consequence of such laws is that they create a 'denial of territoriality' i.e. the attempt to exercise control over persons, situations or areas outside the controller's territory"[51]. Traditionally, these laws are acceptable in exceptional circumstances only[52].

There are not clear sufficient rules in international law govern jurisdictional rules, and all what we have are headlines without enough details, such as sovereignty principle which considered a limitation on the exercise of jurisdiction outside borders. Even international law cases haven't provided clear details about extraterritoriality.

According to international law, the sovereignty principle underscores the exclusive right to exercise certain power within its bounds. This principle is mostly rooted in customary international law, such as 1648 Westphalia treaties and is also referenced in certain international frameworks like the 1945 United Nations charter[53]. Due to the limited body of international case law, the 'Lotus case' is still considered as foundational source base for deriving general principles governing jurisdiction. Three important principles established by the case. The first principle is the issue of extraterritorial jurisdiction is a matter of international law, and states don't have the freedom to extend their jurisdiction unilaterally. Second, International law, generally, prohibits enforcement jurisdiction, unless it is specifically permitted. The last principle is related to extraterritorial prescriptive and adjudicative jurisdiction, which is only permitted if there is sufficient connection between the forum and the event. However, regarding the third point, Kamminga believes that state practice has taken a different

[49] Article 29 Data Protection Working Party, 4.

[50] Microsoft Corp. v. United States, 586 U.S. (2018).

[51] Wissame En-Naoui – Laurence Bégou: How Extraterritorial Laws Impact Your Organization's Sovereignty. *Atos*, accessed February 19, 2024. https://atos.net/en/lp/digital-sovereignty-cybersecurity-magazine/how-extraterritorial-laws-impact-your-organizations-sovereignty#_ftn3.

[52] Menno Kamminga: Extraterritoriality. In: Rüdiger Wolfrum (ed.): *The Max Planck Encyclopedia of Public International Law.* Oxford University Press, 2020. 3. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1040.

[53] William Julie – Sophie Menegon – Alice Murgier: United States extraterritoriality. European Union sovereignty at stake. Accessed February 19, 2024. https://www.ibanet.org/article/CF85E59E-6564-4AA3-9408-3F47C6449C9D.

approach and denies any such jurisdiction unless there is a rule in international law allows that[54]. But reality shows otherwise, there may have been a recent trend in international law to accept this kind of jurisdiction with passive personality[55]. In the Democratic Republic of the Congo v. Belgium Arrest Warrant Case, Judges Higgins, Kooijmans and Buergenthal noted in their combined individual judgment that "the movement is towards bases of jurisdiction other than territoriality"[56]. Based on the two aforementioned cases, the extraterritorial prescriptive and adjudicative jurisdiction are acceptable at least in certain circumstances and the territoriality is no longer the only principle for asserting jurisdiction. However, the new era of the internet has exacerbated the uncertainty of jurisdiction even more and the inherent nature of the internet necessitates more cross-borders legislations. Nowadays, technology laws have extraterritorial effects, and it is understandable that this is unavoidable. Therefore, the question is not whether it's allowed to have these laws or not, rather the question concerns the extent of extraterritoriality, to what extent these laws contain limitations on their scope and what is the level of states' respect to the sufficient connection principle. Additionally, the issue of enforcement and whether states have entered into mutual agreements for judgment enforcement is crucial, as it is clear that in the absence of international rules, the lack of mutual enforcement agreements makes the enforcement of courts' judgments impossible.

In the following paragraphs, we will explore examples of laws and case laws from various countries that have extraterritorial reach, highlighting the disparities between them, in terms of their scope of cross-border application.

Certain EU countries' court cases have applied their laws with extraterritorial effect. For instance, the Paris County Court ruled in a landmark decision that Yahoo! Inc., a US-based company, was subject to French jurisdiction regarding its online auction site, Yahoo Auctions, which featured artifacts associated to the Nazi movement[57]. The court's ruling illustrated the digital age's extraterritorial application of national laws, showing that nations may impose their legal obligations on internet corporations even if they are based abroad.

Google, a US-based corporation, was found to be liable for its search engine results in Spain under the Spanish Data Protection Act (LOPD) by the Court

54 Kamminga 2020, 7-9.
55 Kolossa 2016, 800.
56 Kamminga 2020, 7-9.
57 League Against Racism & Antisemitism v. Yahoo! Inc. & Yahoo France, Paris County Court, Order dated May 22, 2000.

of Justice of the European Union (CJEU). The court's ruling demonstrated the territorial scope of the European Union's (EU) data protection law's[58].

The standards set forth by the EU General Data Protection Regulation (GDPR) go beyond traditional characteristics of natural persons, such as citizenship or place of habitual abode[59].

The Data Security Law of the People's Republic of China[60], PRC Personal Information Protection Law and the 2017 Draft for Public Comments on the Safety Assessment Guide for Data Transferred Outside of China have extraterritorial effects. The guide applies to foreign data controllers or processors who sell goods or services to people in China even though they are not registered in China[61].

The Data Security Law permits its rules to be applied internationally. Legal responsibility must be prosecuted in accordance with the law when data handling operations jeopardize national security, the public interest, or the legitimate rights and interests of PRC residents or organizations. Terms used by the law like national security and public interests are not defined and can be interpreted widely.

Order of the Cyberspace Administration of China No. 4 Article 3 provides for the application of the order to the collection, storage, use, disclosure and exchange of children's personal information via network activities inside the borders of the People's Republic of China[62].

The legal position in the United States is significantly more advanced than that of other nations. The legal position with respect to internet jurisdiction in the country has evolved through multiple levels in courts through several tests[63]. Businesses operating in several jurisdictions may be subject to both federal and state data protection laws about their operations that impact citizens of the United States. These rules apply in situations where the company gathers, saves, sends, handles, or distributes personal data about people living in the United States.[64]

58 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Court of Justice of the European Union (CJEU), Case C-131/12, Judgment of 13 May 2014.

59 Jie Jeanne Huang: Applicable law to transnational personal data. Trends and dynamics. *German Law Journal*, 6/2020, 1283–1308. 1297.

60 Data Security Law of the People's Republic of China, adopted on June 10, 2021, and promulgated on September 1, 2021.

61 Huang 2020, 1297.

62 Order of the Cyberspace Administration of China No. 4, Provisions on the Cyber Protection of Children's Personal Information (Aug. 22, 2019, effective Oct. 1, 2019).

63 Vaishnavi 2023, 4.

64 https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

The CLOUD Act[65], enacted as result of the Microsoft case, expanded the US government's ability to access data abroad and allowed the government to enter into executive agreements with other governments for cooperation in criminal investigations. The act raised concerns about data violation alongside jurisdictional challenges. Simply by having a subsidiary in the USA, a foreign company can be subject to US jurisdiction. Its operational ties to the U.S. through an office bring it within the ambit of U.S. law under the CLOUD Act. The purview of this Act includes companies that operate in or with the United States in addition to those with their headquarters there. Moreover, the CLOUD Act may extend its extraterritorial reach to any entity that makes use of services having a direct or indirect corporate link to the United States. Therefore, the United States has jurisdiction over a foreign business's U.S.-based operations or links, rather than the foreign firm itself[66]. As for the crimes the cloud covers, the cloud mentions (serious crimes) and without any further explanation[67].

The Children's Online Privacy Protection Act of 1998 (COPPA) in the United States is not limited to U.S. companies but extends its jurisdiction to foreign websites that collect personal information from children on U.S. soil. COPPA applies to companies "located on the Internet", meaning the physical location of the website is irrelevant if it conducts business within the U.S.[68]

According to the California Consumer Privacy Act, companies that gather personal data from Californians and satisfy one of three requirements – namely, having an obvious relationship to the state – come under its purview.

A. Businesses whose total yearly gross revenue as of January 1st of the previous calendar year was more than twenty-five million dollars ($25,000,000).

B. Organizations that purchase, sell, or exchange personal data from 100,000 or more customers or households each year, either singly or jointly.

C. Companies whose sales or sharing of customer personal information generate at least 50% of their yearly income.[69]

65 Cloud Act (Clarifying Lawful Overseas Use of Data Act) was enacted in the United States. Public Law No. 115-141, 132 Stat. 1213 (2018) https://www.eurojust.europa.eu/publication/cloud-act#:~:text=The%20Clarifying%20Lawful%20Overseas%20Use,the%20context%20of%20criminal%20investigations. Accessed by February 2, 2024.

66 European Union Agency for Criminal Justice Cooperation. "The CLOUD Act". Last modified December 22, 2022. https://www.eurojust.europa.eu/publication/cloud-act. Accessed February 25, 2024.

67 Ibid.

68 Article 29 Data Protection Working Party, 4.

69 California Legislature (2018). California Consumer Privacy Act of 2018, § 1798.105. Cal. Civ. Code. [2/1/2024, Codes Display Text (ca.gov)].

India is not exempt from extraterritorial effect laws. Clause 75 of the Information Technology Act, subject to certain restrictions, extends its application to any person, regardless of nationality, for offenses or violations committed outside the borders of India. The act is applicable if the behavior or acts that constitute the violation include a computer, computer system, or computer network located inside the borders of India[70], it is based on effects test.

The Delhi High Court used the effects test and determined whether the website was interactive in the cases of India TV Independent News Service Pvt. Ltd v. India Broadcast Live Lic, and Banyan Tree Holding Pvt Ltd v. A Murali Krishna Reddy.[71]

Greek law used to extend the Data Protection Authority over data controllers outside of Greece who processed data on Greek residents by requiring them to appoint a representative in Greece who would be liable for such data processing. The Greek provision was changed in 2006 following objections by the European Commission.[72]

Other law examples that have extraterritorial effect are: Hessisches Datenschutzgesetz of 30 September 1970 (Data Protection Act of the German federal state of Hessen); Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (French Act N. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties); Swedish Data Protection Act of 11 May 1973[73].

In the absence of universally binding regulations, the existence of these laws becomes inevitable, particularly in the realm of online transactions. The practices of various states indicate a degree of recognition of this trend, potentially elevating it to the status of international customary law. This issue is no longer about questioning the legitimacy of such laws; instead, it revolves around establishing clear boundaries for their scope.

5. Disparity in degrees of extraterritoriality

While these laws have extraterritorial effects, they are not all to the same degree. There is variation between them, some of which include conditions that may restrict their scope and making them more acceptable than others.

[70] The Information Technology Act, 2000 (No. 21 OF 2000).
[71] Vaishnavi 2023, 5.
[72] Kuner 2010, 188-189.
[73] Ibid. 176.

In China, both of the Data Security Law of the People's Republic of China[74] and the PCR's Personal Information Protection Law[75] have provisions with extraterritorial effect similar to GDPR, however with certain differences.

Guidance on understanding the notion of offering goods or services can be found in Recital 23 of GDPR. It highlights that merely having contact information or a website accessible within the Union is not enough to ascertain such intent. Nonetheless, a controller's purpose to provide goods or services to data subjects in the Union may be indicated by actions like utilizing currencies or languages that are frequently associated with Member States, allowing orders in those languages, or mentioning users or customers within the Union.

A similar requirement can be found in Article 15 of Regulation 44/2001, known as the Brussels Regulation[76], in that context, a joint declaration by the EU Council and the Commission states that *"the mere fact that an Internet site is accessible is not sufficient of Article 15 to be applicable"*.[77] Thus, the mere availability or accessibility of a particular business online, does not qualify it to be considered as sufficient under the regulation and comes into conflict with article 3(2) of GDPR.[78]

In contrast to GDPR, Samuel Yang believes that the wording of PIPL Article 3(2)(I)[79] implies that regardless of whether they originally intended to target Chinese consumers with their offers, any foreign data controller or processor that sells goods or services to individuals in China and processes that individuals' personal information may be subject to the PIPL.[80]

And while Recital 24 of the GDPR describes data subject monitoring as following someone online, which may result in decision-making and profiling based on personal information, Samuel Yang believes that article 3(2)(b) of the

74 Data Security Law of the People's Republic of China, adopted on June 10, 2021, and promulgated on September 1, 2021.

75 PRC Personal Information Protection Law (Final), adopted on August 20, 2021, and effective from November 1, 2021.

76 Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. Official Journal L 12, 16 January 2001, 1-23.

77 The GDPR's Reach, Material and Territorial Scope Under Articles 2 and 3, WR LLP, 2017. https://www.wileyrein.com/newsroom-newsletters-item-May_2017_PIF- The_GDPRs_ReachMaterial_andTerritorialScopeUnderArticles_2_and_3.html.

78 Amogh Mittal: Territorial Jurisdiction of GDPR and Its Application in India. *International Journal of Law Management & Humanities*, 2/2019, 124–127. 126.

79 PRC Personal Information Protection Law (Final), 2021.

80 Samuel Yang: A Look at the Extraterritorial Applicability of China's Newly Issued PIPL. A Comparison to the EU's GDPR. *International Association of Privacy Professionals, 2020.* Accessed February 8, 2024. https://iapp.org/news/a/a-look-at-the-extraterritorial-applicability-of-chinas-newly-issued-pipl-a-comparison-to-the-gdpr/.

draft PIPL, broadens the definition to cover foreign processing operations that assess and analyze people's conduct in China. This broader terminology may include any type of analysis, evaluation, or study of people's conduct in China in addition to the monitoring activities specified in the GDPR[81].

PIPL extends its application even more to reach "other circumstance as provided by any law or administrative regulation". This is indicating an open-ended list of possible cases for extraterritorial application.

The formation of jurisdictional rules in the United States has been profoundly affected by prior court decisions. The minimum contact standard was established by the seminal decision of International Shoe Co. v. Washington. It requires a certain degree of interaction with the jurisdiction for a court to assert its jurisdiction without having to be a resident. After that, Hanson v. Denckla established the condition for purposeful availment, which states that a party must have intentionally got engaged with the state; limited contact is not adequate. These ideas were then further developed in Zippo Manufacturing Co. v. Zippo.com, which distinguished between passive and interactive internet activity for the purpose of establishing jurisdiction. These three principles limit the extraterritorial reach of laws and present a positive solution in this regard.

However, other laws adopted a broad approach and extended the scope and reach of their application. For example, the CLOUD Act allows the United States to compel companies under its jurisdiction to disclose any data, regardless of its origin. The law extends its application to third parties, which include both the controller and processor on one hand, and data subjects on the other. If a citizen's data in the EU has been collected by an entity in the EU and later stored its data with a cloud company in the USA, this connection can trigger the application of the USA's CLOUD act on that EU entity and its stored data, which means the law is applied to what I term as (passive parties). Regarding crimes covered by the act, it applies to serious crimes, without any definition to it. Similarly, certain terms used by the Chinese Data Security Law without providing clear definition, such as national security and public interests, so they can be interpreted widely.

Undoubtedly, the challenges posed by the rapid development in cyberspace have made it difficult to confine the applications of domestic laws within a state's borders, and the increasing rate of laws with extraterritorial effects has become unavoidable. The problem now is extraterritoriality without any limitations, when laws assert jurisdiction over any website displayed on computers inside the country without any specifications or limitations. These laws can be generally accepted when demonstrating a state's connection with the persons or

[81] Ibid.

circumstances it intends to regulate[82]. In other words, these laws are somehow tolerated when states show connections to cases reached by their laws. According to section 421 of the restatement (third) of foreign relations, a state may assert jurisdiction when the connection warrants such action. This implies weighing domestic interests against international legal principles such as respecting the sovereignty of other states.

Principles used in cases in the USA can limit the extraterritorial reach of jurisdiction to a reasonable degree. Other more nuanced approaches have a positive effect, such as those outlined in Recitals 23 and 24 of the GDPR, which focus on a controller's intention to offer goods or services to data subjects and use criteria like currencies or languages associated with specific member states. Additionally, the Brussels Regulation used the same language, it asserts that merely having an online presence is not enough to subject a business to a specific jurisdiction.

China's Personal Information Protection Law applies to anyone providing services to its citizens, regardless of the purpose or active/passive nature of their online presence. This absoluteness can lead to the extension of the law's reach.

Indeed, the mere existence of laws with cross-border effects is sometimes problematic, as not all states have mutual agreements. For example, China is not recognized by the EU Commission for providing adequate protection. Additionally, there is a lack of mutual judicial assistance between the EU and China. In most cases, China doesn't recognize the jurisdiction of EU data protection authorities and courts. Moreover, the reluctance of Chinese to acknowledge and enforce court decisions could continue in the Chinese judicial system for a considerable time[83]. Therefore, the EU's inability to enforce its laws in China raises doubts about the efficacy of its data protection legislation.

To sum up, when it comes to data protection jurisdiction, two interests are at stake: privacy and human rights on one hand, and state sovereignty on the other. Jurisdiction forms part of a state's sovereignty, its right to regulate its own public order.[84] Since the issue relates to sovereignty, public international law must govern the matter, especially given that human rights and jurisdiction are both components of public international law. Therefore, jurisdiction in the context of data protection law should be evaluated by the rules of public international law, as it was argued by 'Lotus case' and has been asserted by Article 29 Working Party.

[82] Julie – Menegon – Murgier, Ibid.

[83] Chicago 17th ed. Bo Zhao – Weiquan Chen: Data Protection as a Fundamental Right. The European General Data Protection Regulation and Its Exterritorial Application in China. *US-China Law Review*, 3/2019, 97–113. 109.

[84] Kolossa 2016, 779.

There are fine lines between different interests of states, and the issue of balance is sometimes problematic. Restricting states' ability to extend their jurisdiction beyond their borders could undermine data protection rights and sovereignty. Conversely, granting states the right to extend the effects of their laws outside its borders may violate other states' sovereignty and access peoples' data outside their jurisdiction. For this end it is crucial to find a precise and fair balance between these two opposite interests. Additionally, data collection is not only a human rights concern but also a security concern, as other states could potentially use this data in ways that harm others.

6. Conclusion and recommendations

Data protection is recognized as a human right, and it is a multifaceted issue. Governments, while claiming to expand their jurisdiction for the protection of their citizens' privacy, often violate it for their own interests and may persecute internal opponents. Therefore, maintaining a balance between conflicting interests remains delicate and challenging. The issue becomes more complex when it collides with sovereignty, and other interests overlap, such as protecting national security, leading to more complexity of the issue and ultimately making it difficult to achieve a balance. Anyway, the study focused more on jurisdiction and sovereignty concerns, in addition to the possibility of conflicting laws. Jurisdiction, which is essentially the legitimate power a state possesses to act in a given matter, is a cornerstone of sovereignty, should be governed by public international law, as highlighted by the Lotus case and article 25 of the working party. However, there is almost a lack of unified rules in international law regarding jurisdiction, especially in data protection. Presently, international law cases offer only specific guidelines, notably from cases like Lotus. According to this case, states can extend their jurisdiction beyond their borders in the absence of prohibitive rules, provided there is a connection between the forum and the case.

Moreover, the widely repeated states practice enacting laws with extraterritorial effect, suggesting a tolerant attitude towards such legislations. However, with the rise of internet technology, physical borders have become less relevant, promoting states to safeguard their citizens' data and national security with more vigilance. While these laws are generally tolerated, the concern lies in the absolute nature of some of them, and lacking limitations on their scope, such as requiring minimum contact or the explicit targeting of individuals' data. Now the problem is with the extent to which states extend their jurisdiction and to what extent they put limitations on the extraterritorial reach of their data laws.

The absence of comprehensive international law rules leads to states extending the power of their laws according to their interests, often without considering the consequences. Consequently, companies and websites may find themselves subject to multiple jurisdictions simultaneously, creating potential conflicts of laws and legal uncertainty for websites.

Recommendations

- Establishing a unified international legal framework to govern jurisdiction in cyberspace generally and data protection specifically.
- While achieving binding rules is challenging, promoting soft law – nonbinding declarations – is crucial.
- Any international rules should strike a balance between the legitimate concerns of nations regarding their national security and peoples' data on one hand, and the respect of the sovereignty of other states from the other.
- Laws with extraterritorial effects should include specific limitations, such as sufficient connection to the forum and the specific intent to target individuals within their jurisdiction.
- To avoid their misinterpretation, vague terms such as 'national security' should not be left without clear boundaries.
- The application of extraterritorial laws should be confined only to third parties with minimal connection, and not to people with a passive connection, or what I term 'passive parties', as seen in the US CLOUD act.

Bibliography

Court cases

Hanson v. Denckla, Supreme Court of U.S., https://law.justia.com/cases/federal/district-courts/FSupp/952/1119/1432344/ Accessed by 5/2/2024.

Microsoft Corp. v. United States, 586 U.S. (2018).

Legal documents and regulations

Stephan Kolossa: The GDPR's Extra-Territorial Scope. *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 4/2020, 791–818.

Regulation (EU) No. 1215/2012 of the European Parliament and of the Council, of 12 December 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

Geneva Round Table on the Questions of Private International Law raised by Electronic Commerce and the Internet, organised jointly by the University of Geneva and the Hague Conference on Private International Law, Geneva, 2-4 September 1999.

The Internet and Jurisdiction Policy Network released their first-ever Global Status Report in Berlin on 27 November 2019.

Order of the Cyberspace Administration of China No. 4, Provisions on the Cyber Protection of Children's Personal Information (Aug. 22, 2019, effective Oct. 1, 2019).

European Union Agency for Criminal Justice Cooperation. "The CLOUD Act". Last modified December 22, 2022. https://www.eurojust.europa.eu/publication/cloud-act. Accessed February 25, 2024.

California Legislature (2018). California Consumer Privacy Act of 2018, § 1798.105. Cal. Civ. Code. [2/1/2024, Codes Display Text (ca.gov)].

Data Security Law of the People's Republic of China, adopted on June 10, 2021, and promulgated on September 1, 2021.

PRC Personal Information Protection Law (Final), adopted on August 20, 2021, and effective from November 1, 2021.

Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. Official Journal L 12, 16 January 2001.

Journal articles

R. Vaishnavi: Internet and Jurisdiction. Global Status. *Indian Journal of Law and Legal Research*, 5/2023, 1–9.

Joanna Kulesza: Transboundary Challenges to Privacy Protection in Cloud Computing. *Ukrainian Journal of International Law*, 2/2017, 117–128.

Kai Burmeister: Jurisdiction, Choice of Law, Copyright, and the Internet. Protection against Framing in an International Setting. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 2/1999, 625–723.

Krzystof Zalucki: Extraterritorial Jurisdiction in International Law. *International Community Law Review*, 4-5/2015, 403–412.

Christopher Kuner: Data protection law and international jurisdiction on the Internet (part 1). *International Journal of Law and Information Technology*, 2 /2010, 176–193.

Stephen Kobrin: Safe Harbours Are Hard to Find. The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance. *Review of International Studies*, 1/2004, 111–131. http://www.jstor.org/stable/20097901.

Recommendations and guidelines

OECD, Recommendation of the Council on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. OECD/LEGAL/0352 Retrieved from https://www.oecd.org/digital/privacy/ : https://www.oecd.org/digital/privacy/.

OECD, Digital Economy Papers. No. 360, "Explanatory Memoranda of the OECD Privacy Guidelines". 2023.

Reports and working documents

Amnesty International, Universal Jurisdiction. 4. https://www.amnesty.org/en/wp-content/uploads/2021/06/ior530032001en.pdf (accessed October 12, 2023).

Article 29 Working Party: Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites' Brussels - Belgium 2/2002.

The Internet and Jurisdiction Policy Network released their first-ever Global Status Report in Berlin on 27 November 2019.

Websites and other sources

Betsy Rosenblatt: Principles of Jurisdiction. *Berkman Klein Center for Internet & Society at Harvard University*. https://cyber.harvard.edu/property99/domain/Betsy.html.

Wissame En-Naoui – Laurence Bégou: How Extraterritorial Laws Impact Your Organization's Sovereignty. *Atos*, accessed February 19, 2024. https://atos.net/en/lp/digital-sovereignty-cybersecurity-magazine/how-extraterritorial-laws-impact-your-organizations-sovereignty#_ftn3.

Menno Kamminga: Extraterritoriality. In: Rüdiger Wolfrum (ed.): *The Max Planck Encyclopedia of Public International Law.* Oxford University Press, 2020. 3. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1040.

EXPLORING THE HISTORICAL ROOTS OF HUMAN TRAFFICKING, OR THE STATUS OF SLAVES IN ANCIENT ROME

DÁNIEL SZŰCS[1]

ABSZTRAKT ■ Jelen tanulmány a római rabszolgaság intézményének történelmi mélységeibe hatol annak érdekében, hogy feltárja az emberkereskedelem bűncselekményének gyökereit. Az egyes aspektusok boncolgatásával a szerző arra törekszik, hogy fényt derítsen a kizsákmányolás tartós örökségére, s egyben lehetőséget biztosítson annak megvitatására is, hogy az ókori tradíció miként vált évezredek alatt az emberkereskedelem alapvető emberi értékekkel össze nem egyeztethető bűncselekményévé, amely napjainkban is sújtja a világot. Kulcsfontosságú kiindulópontként tekinthetünk arra, hogy a rabszolgaság szerves részét képezte az említett ókori társadalomfelfogásnak. Az egyben társadalmi, kulturális, és gazdasági dimenzió feltárásával a tanulmány arra a szisztematikus dehumanizálásra kíván rávilágítani, amelyet az ókorban szenvedtek el a rabszolgák. Az értekezés a római rabszolgaság kulcsfontosságú aspektusait veszi górcső alá, melyek közül példaként említhető az egyes személyállapotot érintő kérdések, a rabszolgaság keletkezési és megszűnési módozatainak széles spektruma, az olykor embertelen életkörülmények, valamint az állam és a társadalom szerepe az intézmény állandósításában. Amennyiben párhuzamot kívánunk vonni a rabszolgákkal való bánásmód és az emberkereskedelem mai áldozatainak helyzete között, megállapíthatjuk, hogy a múlt meglehetősen nagy árnyékot vetít a jelenkorra. A történelmi vizsgálat célja, hogy felhívja a figyelmet az emberkereskedelem tartós jellegére, s folyamatos éberségre, cselekvésre szólítson fel az emberi jogok megsértése elleni örökös küzdelem jegyében.

ABSTRACT ■ This paper delves into the historical depths of the institution of Roman slavery in order to explore the roots of the crime of human trafficking. By dissecting each aspect, the author seeks to shed light on the enduring legacy of exploitation, while also providing an opportunity to discuss how the ancient tradition has evolved over millennia into the crime of trafficking, incompatible with fundamental human values, that continues to plague the world today. A key starting point is that slavery was an integral part of this ancient social concept. By exploring the socio-cultural, economic and social dimensions, this study aims to highlight the systematic dehumanisation that slaves suffered in antiquity. The thesis focuses

[1] PhD Student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

on key aspects of Roman slavery, such as issues of personal status, the wide spectrum of ways in which enslaved status arose and ended, the sometimes inhumane living conditions, and the role of the state and society in perpetuating the institution. Drawing parallels between the treatment of slaves and the situation of victims of trafficking today, the past casts a rather large shadow over the present. The aim of the historical inquiry is to draw attention to the persistence of human trafficking and to call for continued vigilance and action in the perpetual struggle against human rights violations.

Keywords: exploitation, inhuman treatment, forced labour, trafficking in human beings, slavery

1. Preface

Today, we take a legal constellation for granted whereby the whole legal system is permeated by the acquis of equality before the law. However, looking at the different periods of history, this is far from being a permanent phenomenon, and it has been a rather bumpy – and in many cases ruthless, with no regard for dozens of human lives – road to this advanced concept. In the words of Ágnes Czine,[2] *"trafficking in human beings in the 21st century is the cruellest violation of human rights from the perspective of the victims."*[3] This segment of crime is the third largest and fastest growing industry in the world, keeping millions of people in 'slave conditions'.[4] The existence of slavery is as old as our history. The phenomenon of human trafficking is often referred to as modern-day slavery.[5] Szandra Windt points out that *"traffickers treat their victims as 'slaves' for both sexual and labour (sometimes other) purposes, taking advantage of their vulnerable position"*.[6] However,

2 Ágnes Czine: *Az emberkereskedelem, mint a szervezett bűnözés egyik megjelenési formája*. Pécs, s.n., 2011. 13. https://pea.lib.pte.hu/handle/pea/15593.

3 On the conceptual aspects of victim, see: Andrea Domokos – Renáta Garai: A bűnözés és a büntető igazságszolgáltatás áldozatai. *Glossa Iuridica*, 2019/3-4. szám, 9–22.; Andrea Domokos: Az új Büntetőeljárási Kódex sértettekre vonatkozó egyes rendelkezéseiről. *Glossa Iuridica*, 2018/3-4. szám, 137–148.; Andrea Domokos: *Büntető anyagi jog – általános rész*. Budapest, Patrocinium Kiadó, 2019. 37.

4 Czine 2011, 13.

5 See: Miklós Hollán: Az emberkereskedelem büntetni rendelése a nemzetközi instrumentumok tükrében. *Állam- és Jogtudomány*, 2007/2. szám, 273-287.; Miklós Hollán: Az emberkereskedelem tényállásának jogharmonizációja az európai unióban. *Büntetőjogi Kodifikáció*, 2008/2. szám, 22–26.; Szandra Windt: Gondolatok az emberkereskedelemről. *Miskolci Jogi Szemle*, 2019/2. szám, 459–469.; Lenke Fehér: Az emberkereskedelem komplex problémája. *Állam- és Jogtudomány*, 2012/4. szám, 397–420.

6 Windt 2019, 460.

Windt also draws attention to a conceptual distinction based on the fact that the term slavery is often used as a synonym for human trafficking. Though, according to her, the former is a rather broader concept compared to the latter.[7] In this context, Lenke Fehér argues that human trafficking today is to some extent comparable to the slave trade of the past,[8] precisely because the essence of both activities is the treatment and exploitation of human beings as quasi-objects, commodities.[9] In my view, Szandra Windt's statement did not place the two concepts in an alternative context, but merely highlighted the logical direction from less to more, and that these two concepts are not completely equivalent. Lenke Fehér complements this line of thought when she establishes the similarity between the two concepts on the basis of the essence of activity. Trafficking in human beings, having regard to its criminal character, necessarily presupposes illegality. In contrast, slavery, some aspects of which correspond to the conceptual elements of contemporary human trafficking, was not criminalised in any historical period, as we will see later in this paper. In view of this, the above two theses – one might say hand in hand – do not contradict each other, rather they reinforce each other. According to Károly Kubisch, the complete abolition of slavery is still not a reality, since despite the prohibition of the Christian creed, traces of the 'frenzies' of the Dionysian and Bacchanalian can be found in our culture.[10] If these assertions are to be accepted as true, then in order to credibly examine aspects of 21st century human trafficking[11] in the future, it is first necessary to recall the past and historical significance of slavery, which has its roots in ancient Rome. This study attempts to provide an overview of the situation of Roman slavery along certain social and legal lines. The author seeks to answer the question of how we might view the above-mentioned period of history, which is gloomy in this respect, in the light of contemporary legislation, which focuses on human rights and protects them through criminal law.

We can agree on the fact that slavery was an integral part of both Roman culture[12] and law, and therefore we can see the imperial legacy as a slave-owning society, while of course laying the foundations of a continental legal system that established millennia of tradition and maintained intellectual community

7 Ibid. 460.

8 Conf. Ferenc Bajusz: *Az ókori rabszolgák helyzete és sorsuk alakulása a kereszténység hatása alatt*. Budapest, Budapesti Református Akadémia Kiadó, 1969. 13.

9 Fehér 2012, 397.

10 Károly Kubisch: *Az emberkereskedelem büntetőjogi megítélésének morális és szabályozási változásai*. Budapest, s.n., 2021. 25. https://doi.org/10.24395/KRE.2022.005.

11 Ágnes Czine – Andrea Domokos: *Büntetőjog – Különös rész I*. Budapest, Patrocinium Kiadó, 2017. 93-104.

12 Conf. István Hahn: Az ókori vallások és a rabszolgaság. *Világosság*, 1965/6. szám, 423–441.

in the modern age. However, there is also a view that it is not justified to speak of slave-owning societies, given that a large part of ancient societies basically assumed that work was provided by free people from poorer social classes.[13] The demographics of Rome's slaves are, in the vast majority of cases, not available in the form of precise figures, given the sources that survive. However, in the light of census data from the time of emperor Augustus, three basic demographic views have emerged, in which the number of slaves is estimated based on the total population,[14] bearing in mind the inevitable feature that these counts naturally differ, sometimes significantly. For instance, the population of Italy[15] is estimated at between 5.5 and 14 million at the dawn of the imperial era, with 2 to 4 million slaves.[16] Estimates for Roman Italy assume the presence of slaves in fairly high numbers. The main feature of the aforementioned imperial censuses is that they only list Roman citizens within the total population, which means that we have no direct information on slaves.[17] Scheidel, a prominent scholar of Roman demography, argues in his treatise that the number of slaves in Italy was at most 1.5 million, which makes their social proportion lower than others have estimated.[18] In the urban census lists derived from central Roman Egypt, nearly 15% of the registered people were not free, despite the fact that one in five households had at least one slave.[19] Verboven states[20] that three quarters of the slaves who were finally buried in Roman and Ostian burial grounds were free men, which the Takács–Gacsal pair consider to be an exaggerated proportion.[21]

13 Péter Hahner: *100 történelmi tévhit.* Budapest, Animus Kiadó, 2010. 21.

14 These are the so-called high count, low count and middle count.

15 Conf. Alessandro Launaro: *Peasants and Slaves. The Rural Population of Roman Italy.* Cambridge, University Press, 2011. 14-24.; Géza Alföldy: *Római társadalomtörténet*. Budapest, Osiris, 1996. 70.

16 For other estimates, see: Walter Scheidel: Human Mobility in Roman Italy II. The Slave Population. *The Journal of Roman Studies,* 95/2005, 64–79.

17 The figures are further complicated by the distribution of the population in terms of the so-called *status civitatis*, according to which among the freemen not only the *cives Romani* (Roman citizens), but also the *Latini* and the so-called Peregrinians were present in the territory of Rome. However, the latter did not have legal capacity under imperial law, although they were free.

18 Scheidel 2005, 64.; conf. Morris Silver: Contractual Slavery in the Roman Economy. *Ancient History Bulletin*, 25/2011, 73–132.

19 Scheidel 2005, 66.

20 Koenraad Verboven: The Freedman Economy of Roman Italy. In: Sinclair Bell – Teresa Ramsby (ed.): *Free at Last! The impact of freed slaves on the Roman Empire*. London, Bloomsbury Publishing, 2011. 90.

21 Levente Takács – Dóra Gacsal: A római rabszolgaság. *Korall*, 2016/63. szám, 54–68.

2. Introduction to the personality rights

In classical Roman law,[22] people (homines) were divided into free men (liberi) and slaves[23] (servi) based on the status libertatis.[24] From a dogmatic point of view, only the free were explicitly considered as persons, distinguishing between those who were born free (ingenui) and those who were liberated later (libertini). Consequently, it appears contra legem that slaves could not be considered persons, and were in fact considered by law to be things.[25] The precise elaboration of advanced ancient law is faithfully reflected in the fact that, although the servant was regarded as equivalent to a domestic animal according to certain classifications of things, it was not regarded as a thing in the ordinary sense, so that the servi's humanity was to some extent recognised in legal terms.[26] In view of this, the power of ownership over the slave was not called the right of property (domicinium), but rather so-called slaveholder ownership (dominica potestas).[27] The servi, however, was not a legal entity, rather a legal subject[28] in Roman law, whereby the master not only kept him under his power, but also forced him to work (forced labour), sold him, traded him, and sometimes even killed him.[29]

3. Must be born to be a slave?

In the following, I will take the forms of slavery's origin and termination under the lens of the imaginary magnifying glass what I use as a tool of my research. In response to this proposition, it is clear from the outset that not everyone was born to be a slave in antiquity, many of them became slaves over time, depending on other circumstances.[30] The first and most obvious way for slavery to come about was when at the end of fighting conflicts, losers who survived the battle

22 Paul. Dig. 4,5,11.

23 Ulp. Dig. 50,17,22.

24 Gai. Inst. 1,9. *„Et qiudem summa divisio de iure personarum haec est, quod omnes homines aut liberti sunt aut servi."*

25 Ulp. 19,1. *„Servi res sunt."*

26 András Földi – Gábor Hamza: *A római jog története és institúciói*. Budapest, Nemzeti Tankönyvkiadó, 1996. 212.

27 Ibid. 203, 205, 212.; Róbert Brósz – Elemér Pólay: *Római jog*. Budapest, Nemzeti Tankönyvkiadó, 1974. 132, 138.

28 I note marginally that here we can already feel the fundamental violation of humanitarian law and the duality of interpretation of the concept of person-thing, given that man cannot be identical with the physical thing by definition.

29 By definition, property right can be understood as free disposition of property.

30 Inst. 1,3,4. *„Servi autem aut nascuntur aut fiunt."*

were taken captive.[31] The process was triggered by the communes' recognition that they could increase the human resources needed for their work primarily not only by their own strength, but consequently also by the non-fallen fighters from the enemy camp. Therefore, it was considered more economical and socially valuable to spare their lives and employ them than to deprive them of the eternal light. In view of this, the historical roots of the origins of slavery are essentially to be found in the war captivity. Along this line, Brósz and Pólay point out that a citizen of a state which was hostile to Rome was considered an enemy who could be freely captured. It may therefore be possible to enslave a foreigner not only when he was a prisoner of war, but also when he was taken into captivity in Rome in 'peacetime', not as a combatant.[32] Furthermore, we can also argue that the state used the slaves who were ordered to forced labour[33] to fulfil certain state purposes on the basis of the ius gentium, while others ended up in private ownership. Those in the former category had an advantage over backyard slaves in that they could live in a marriage-like relationship with a free woman and could decide about half of their peculium in a will.[34] People who came into the world as the children of a woman in slavery,[35] became slaves from birth. I find it necessary to mention here the principle of favor libertatis.[36] The essence of this principle was that if the mother was liberated for even a moment during her pregnancy, her child born alive was considered free, regardless of the fact that the mother might be enslaved again.[37] The third form of the origin of slavery was the enslavement of free man by punishment. The highest degree of change of status[38] (capitis deminutio maxima)[39] was imposed on anyone who, on the one hand, had exempted themselves from the census (incensus) and, on the other hand, had escaped from military service or deserted while on duty. This latter

31 Takács – Gacsal 2016, 4. Conf. Ferenc Réthey: *A római rabszolgaság*. Kecskemét, Szél Nándor Nyomda, 1913. 20-21. During the Second Punic War, when the city of Tarentum fell, the Romans enslaved nearly 30,000 people.

32 Brósz – Pólay 1974, 138.

33 *Servi publici*.

34 Brósz – Pólay 1974, 139.

35 Partus ancialle.

36 Its importance is underlined by Paul. Dig. 50,17,106. *„Libertas inaestimabilis res est."* (Transl.: Freedom is a priceless asset.); Gai. Dig. 50,17,122. *„Libertas omnibus rebus favorabilior est."* (Transl.: Freedom comes before everything else.).

37 Paul. Sent. rec. libri V. 2,24,1-3.; Marc. Dig. 1,5,5,3.

38 Paul. Dig. 4,5,11.

39 The capitis deminutio maxima is the most complete (negative) change (reduction) in the status of a person, which affects freedom, property and thus legal capacity in its entirety, with the person concerned being deprived of all these and reduced to a state of servitude.

was sold as a slave, deprived of all his property, so-called trans Tiberim.[40] If the debtor citizen could not pay the creditor because he had become insolvent, his creditor could make him his own slave by manus iniectio. But Roman law also recognised other forms of enslavement. A free man could also sell himself into slavery at his own free will.[41] According to Pratorian law, a person who had previously been a slave but had been liberated, could be enslaved again - by being recalled by his former slaveholder - if he had behaved ungratefully after his manumission. A free woman who, in violation of another's property rights, had sexual intercourse with his slave, and the slave did not stop despite the lord's protests,[42] was also forced into servitude under the[43] Senatus Consultum Claudianum.[44]

4. The way out of slavery

Let us take a look at the diversity of the termination of slavery also. A way out of slavery was essentially the legal institution of manumission. Within the conceptual category of civil law, we can distinguish three categories of cases. [45] Firstly, we can talk about the manumissio vindicta, which was a pro form trial before the praetor.[46] A person could become a free man secondly if he was listed in the register of Roman citizens (census), and also if his lord (slaveholder) declared him free by testamentary will (manumissio testamento).[47] In addition to these rules, praetorian law has also developed additional cases, such as release in

40 I.e. "beyond the Tiber"", means abroad. This form of debt slavery was abolished by law in 326 BC. Conf.: Egon Maróti: *Rabszolgák az ókori Rómában*. Budapest, Gondolat Könyvkiadó, 1969. 54.

41 Ulp. Dig. 21,1,17,12.; Ulp. Dig. 28,3,6,5.

42 Paul. Sent. rec. reg. 2,21a.

43 54 AC.

44 Földi – Hamza 1996, 213-214.; Brósz – Pólay 1974, 137.

45 The three categories of civil rights were supplemented in the late imperial period by the manumission in the church (manumissio in ecclesia).

46 This suit for liberty was feigned because one of his confidants brought a suit before the praetor against the person who wished to be freed. In doing so, he held out his wand (vindicta) to the slave and made a declaration of rights declaring that the slave was free. The master then released the servant (manu mitti) from his hands, at the same time the praetor declared him free.

47 The Lex Fufia Canina limited emancipation by will to the number of slaves in Augustus' time.

front of friends, [48] by issuing a letter of liberty,[49] or by sitting at the lord's table.[50] However, the liberation was far from unlimited.[51] For mention's sake, the lex Aelia Sentia prescribed that a lord under the age of 20 could not liberate a slave and a slave under the age of 30 could not be liberated.[52] The legal institution of amnesty was also known by the Romans in the sense that a slave could be freed not only by his lord as a natural person, but also by the state in certain cases. For instance, if a slave had demonstrated a self-sacrificial behaviour or performed a service of overriding public interest,[53] the state could declare the slave to be free, regardless of the slaveholder.[54]

In addition to what has just been described, there was also a violent form of liberation, namely the slave revolt, in which the subordinate gained de facto independence but remained de iure a slave. Under a rule dating from the imperial era, slavery could end if the subject had lived free in good faith for 20 years.[55] However, in the case of slave revolts, this rule is far from being applicable, because even if the 20 years have elapsed, good faith is conceptually excluded due to the intentional, violent, unlawful conduct, so that manumission is not possible. The number of slaves grew massively in ancient Rome in the classical era.[56] As a result, the servi, who in the Patriarchal period had a similar status to a child of the household, had already become distant from his lord by the Classical period, so for this reason a significant social differentiation can be observed. The vast majority of slaves were forced to work in miserable, inhumane conditions. The picture is nuanced by the different standards of living that different rulers have provided for slave labourers throughout history.[57] The image of their social 'degradation' in the classical period is reinforced by the senatus consultum Silanianum, [58] according to which, if the slave owner was a victim of homicide, the other (innocent) slaves

48 Manumissio inter amicos.
49 Manumissio per epistulatum.
50 Manumissio per mensam.
51 Gai. Inst. 1,18-19.
52 Brósz – Pólay 1974, 139–140.
53 For example, he caught a criminal.
54 In imperial times, it was considered common practice to free slaves who, after being sold, were found to have violated the collateral agreement of the contract. The most common example of this was when a slave was sold with the stipulation that he could not be forced into prostitution, but when this happened, the state gave the enslaved person his freedom: mult-kor.hu/milyen-volt-rabszolganak-lenni-az-okori-romaban-20150303?pIdx=4.
55 Brósz – Pólay 1974, 140.
56 Földi – Hamza 1996, 213. Conf. Brósz – Pólay 1974, 138.
57 Réthey 1913, 22.
58 10 AC.

under his authority[59] were also sentenced to death if they did not try to defend their lord by risking their own lives. The 'flowering' of slavery can be considered to be the period that began with the large-scale destruction of the free bourgeoisie after the Second Punic War, and which is essentially connected to the emergence of latifundia and the commodity-producing slave industry. [60] Since the servi was not paid for the work he did, it was cheap, and also because it was under the authority of the lord, i.e. legally depended on him, it was a safe way[61] of cultivating the land. Along these lines, it is not strange to say that one of the most important means of agricultural production in antiquity was the slave.[62]

In the words of Egon Maróti: [63] *"Slaves did an incomparably higher percentage of productive – or essential maintenance, service, etc. – work than free people."* [64] Consequently, slaves were present in almost all areas of contemporary life, which basically involved human effort. In addition to their legal status, the standard of living was the point of significant difference compared to the worldview of the free. The definition of the place of work by the lord also had a major distorting effect on the slaves' existential condition. In this context, we can basically distinguish between two main groups of subordinates.[65] Those who worked in urban houses formed the familia urbana, which included all those who performed personal service around the lord (slave owner) and his relatives.[66] Those working on rural estates made up the other group, the familia rustica. Considering that the work[67] done by the latter was considerably more demanding and the living conditions in the countryside were of a rather lower standard, it could be said that sending someone from the city to work in the countryside was tantamount to a punishment. This is well illustrated by the fact that slaves were considered as 'speaking tools', and therefore as appurtenances to the landed estate.[68] In addition to physical hardship, the subordinates were, with a few refreshing exceptions,

59 Those who live under the same roof (sub eodem tecto) or those accompanying him.
60 Réthey 1913, 20–21.
61 Because of the dependent legal status, the slave did not resist his lord.
62 Éva Jakab: *Humanizmus és jogtudomány. Brissonius szerződési formulái I.* Szeged, Pólay Elemér Alapítvány, 2013. 183.
63 Maróti 1969, 17.
64 Leonhard Schumacher: Slaves in Roman Society. In: Michael Peachin (ed.): *The Oxford Handbook of Social Relations in the Roman World*. Oxford, Oxford University Press, 2011. 594.
65 Réthey 1913, 36.
66 For example, dresser, chef, courtier, room servant.
67 For example, shepherds, gardeners, arable planters, manure bearers. See: Cato, De agr. 2,3-4.
68 Paul. Sent. rec. reg., 3,6,34-37.

[69] tortured, starved, unjustly punished, harassed and even killed at the whim of their lords.[70]

The ruthless treatment and sub-standard living conditions opened the way for a violent escape from slavery, sometimes historic slave rebellions,[71] which were the culmination of the 'golden age'. With the spread of Christianity, a milder period followed, at least reforms were made, with laws banning some or all the practices before. Noteworthy in this context is the Lex Petronia,[72] which forbade owners to throw their slaves in front of wild animals in the arena without the prior permission of the praetor. The Edictum Claudianum liberated the old slave who had been starved by his master. Emperor Hadrian decreed that lords could not kill their slaves with their own hands (see earlier) until the praetor had given his prior permission. Pius Antonius had already given the almost completely disenfranchised the right to complain to the praetor about their owner's cruelty. It also empowered the praetor to order the owner to sell his servant to the highest bidder in case of cruelty. In time, it was possible for the servi to collect peculium. So, what he earned, or what he received as a gift or tip, the servi could already take or even keep for himself, which he could ultimately use to redeem his freedom.[73]

5. Human trafficking or the slave trade in antiquity

Towards the end of the study, it is also worth mentioning slave trade. Basically, the marketplace was the central location in almost all ancient cities, serving both social and commercial functions.[74] The city of Delos became a dominant maritime trading centre in the 2nd century BC,[75] partly due to the declaration of the island as a free harbour in 168 BC, and partly due to the decline of Rhodes. The latter was of great importance because, with the decline, its control over maritime trade was also lost. The direct consequence of this was an increase in pirate activity at

[69] At the same time, Musico, a slave of the emperor Tiberius, performed a rather high-ranking task, for example, he was responsible for controlling the revenues of Gaul, and was allowed to travel accompanied by his slaves. See: CIL. 6,5197.

[70] Gai. Inst. 1,13-15. When it refers to punishments and torture in the context of liberation by the Aelius-Sentius law.

[71] The three major slave uprisings are the First and Second Sicilian Uprisings and the Spartacus Slave Rebellion.

[72] 79 AC.

[73] Edward Westby: The Roman Slave. *The Law Coach* 3, 5/1922, 76-78.

[74] See: William V. Harris: Towards a Study of the Roman Slave Trade. *Memoirs of the American Academy in Rome*, 36/1980, 117–140.

[75] See also, Egon Maróti: A délosi rabszolgapiac és a kalózkodás. *Antik Tanulmányok IX.,* 1962/1. szám, 1–12.

sea, which played a major role in the growth of slave trade along the sea routes. Strabon argues that the pirates mainly transported their prisoners to Delos or Side in Pamphilia for sale, because these ports were the pirates' famous trading posts.[76] Slave trading could take place in several places in Rome according to the instructions of the market inspectors. Éva Jakab examined in detail certain aspects of trade in ancient Rome.[77] According to her thesis, the Campus Martius served as the central market. Additionally, the Castor temple was rumoured to be a place where slaves of poor quality were sold. Female servants were traditionally offered for sale near the Temple of Vesta and on the Via Sacra. Rather expensive luxury slaves were available for purchase at the Saepta shop.[78] According to Plutarch, there was a special market for the physically handicapped,[79] and there was probably also a trading unit near the island of Aesculapius, where sick and aged slaves[80] were sold.[81] So we can see that slave trade was an integral part of everyday life in Rome.

This is borne out by the fact that, in addition to the large number of legal transactions, the contractual practices for this purpose were also quite elaborate. The commercial customs and formulas of the period were specifically researched by Jakab, following Brissonius.[82] As a starting point, we can consider that the warranty for hidden defects permeated legal transactions even in ancient times, according to which the seller guaranteed the defect-free physical condition of the slave.[83] In the course of trade, slave owners promised certain qualities about slaves, their condition, which we call dicta et promissa.[84] The prevailing principle was that the seller guaranteed that the slave being sold was not a thief, had not escaped,

[76] Strab. Geo. 14,3,2. 14,5,2.

[77] Éva Jakab: Kereskedési szokások a régi Rómában. *Acta Universitatis Szegediensis: acta iuridica et politica Szeged* XLIV., 1993/7. szám, 9–31.; Éva Jakab: Stipulationes aediliciae (A kellékhibákért való helytállás kialakulása és szabályai a római jogban). *Acta Universitatis Szegediensis: acta juridica et politica Szeged* XLIV., 1993/7. szám, 85-114.; Éva Jakab: Rabszolgavételek Rómában. In: Károly Tóth (ed.): *Emlékkönyv Dr. Cséka Ervin születésének 70. és oktatói munkájának 25. évfordulójára.* Szeged, Acta Juridica et Politica, 1992. 247–259.

[78] Jakab 1993a, 16.

[79] Plut. De cur. 10.

[80] Wayne Edward Boese: *A Study of the Slave Trade and the Sources of Slaves in the Roman Republic and the Early Roman Empire*. Washington, University of Washington, 1973. 148.

[81] Jakab 1993a, 8-9; 16-17.

[82] See: Jakab 2013.

[83] It meant nothing more than that the seller was liable for the slave's bodily defects largely in the form of stipulation.

[84] However, we must distinguish between mere "praise" statements for which the seller was no longer responsible (e.g. accurate, reliable).

and had no debt arising from delictum.[85] In addition to hidden (physical) defects,[86] they also demanded responsibility[87] for spiritual (psychological) defects.[88] In the context of the dogmatic analysis of the related liability structure, we can also talk about the fact that the implied warranty does not cover bodily defects arising after the object of sale, but they should be interpreted practically in relation to the past, modelled on the noxa solutus. According to Jakab's theses, the law of Aedilis Curilis treated this range of guarantees in an objective sense, in the light of which the seller assumed responsibility, based on the example above, for the fact that the slave had never attempted to escape or steal until the time of sale, so the emphasis of principle was not on standing up for character or quasi-spiritual defects.[89] The opposite view is taken by Gamauf, who argues that weakness of character (e.g. tendency to escape) in itself amounts to a psychological defect and also gives rise to redhibition.[90] Thus, in the context of the contemporary warranty for hidden defects, the slave trader's (seller's) express statements and promises concerning the qualities, condition or lack thereof of the slave being sold were called dicta et promissa. The fact that a thief had stolen from his lord was not part of the obligation to provide information required by the Edict of Aediles and therefore did not have to be disclosed.[91] However, if the seller made an express statement (undertaking) that the slave who was the subject of the transaction was not a thief, he was clearly liable for it. This gives us a picture of the Roman practice according to which the Edict forced the seller to provide certain information. In addition, the buyer could of course inquire about additional features and characteristics from the seller, bearing in mind the fact that defects visible to the naked eye were at the buyer's risk.[92] It was common practice, for example, for the buyer to also question the slave about his name, homeland, place of birth, his age, and even his past.[93] In this context, Gaius also took the position

85 Éva Jakab: *Praedicere und cavere beim Marktkauf. Sachmängel im griechischen und römischen Recht*. München, C. H. Beck Verlag, 1997. 125.

86 E.g. lame, including both permanent and transient (e.g. fever) diseases.

87 On the slave's flaws, see: Ulp. Dig. 21,1,1.; 21,1,4,6.

88 So-called animi vitia.

89 Jakab 2013, 185.

90 Richard Gamauf: *Ad statuam licet confugere*. Frankfurt am Main, Peter Lang GmbH Internationaler Verlag der Wissenschaften, 1999. 110.

91 Marc. Dig. 21,1,52. *„Si furtum domino servus feceria, non est necesse hoc in venditione servi praedicere nec ex hac causa redhibitio est: sed si dixerit hunc furem non esse, ex illa parte tenebitur, quod drxal promisitve."*

92 Our current civil law rule is also based on the practical concept that the buyer has the duty to inspect the slave (goods), to inspect them carefully and to detect visible defects. See: Dig. 21,1,1,6. Ulp.; Dig. 21,1,14,9-10. Ulp.

93 Jakab 1992, 255.

that the seller must stand up for his binding statements.[94] So, if the seller claimed that the slave had a certain characteristic, but the promised characteristic did not correspond to reality, the buyer had the possibility to withdraw from the transaction or to seek a reduction of the purchase price through a lawsuit. In that regard, Jakab shares Haymann's view[95] that liability for dicta et promissa must be regarded as complementary to the Aedilis reporting obligation.[96]

But the responsibility was by no means unlimited. In addition to this, it is also relevant to clarify what pieces of information the seller did not have to provide, bearing in mind that we can also mention statements that fall under the category of laudatio. Following Florentius, the seller was not liable for statements that were merely praise.[97] In view of this, if the seller made general declarations without any specific content, for example, claiming during the bargaining that the slave was honest, beautiful, obedient, he was not obliged to be liable for these declarations, because they fell into the category of nuda laudatio. Ulpianus also took the view that there is no possibility of a suit on the basis of mere praise.[98] However, this situation does not apply in cases where the seller claims a specific characteristic that allows the slave to be sold at a higher value. In this case, as stated above, he had to stand his ground.[99]

6. Summary

It was established in the sense of the above that the social structure and perception of ancient Rome was fully thematized by the slave question.

Slaves have been regarded as commodities throughout history, so to speak, and as a result they have been traded with noble simplicity. One of the main characteristics of slavery is its coercive character, also discussed above, which is achieved institutionally through violence, hence fear of violence, sometimes torture and systematic oppression through psychological terror in addition to

94 Gai. Dig. 21,1,18 pr. *„Si quid venditor de mancipio adfirmaverit idque non ita esse emptor queratur, aut redhibitorio aut aestimatorio (id est quanto minoris) iudicio agere potest."*

95 Franz Haymann: *Die Haftung des Verkäufers für die Beschaffenheit der Kaufsache I. Studien zum klassischen römischen Recht*. Berlin, s.n., 1912. 31.

96 Jakab 2013, 185-186.

97 Flor. Dig. 18,1,43 pr. *„Ea quae commendandi causa in venditionibus dicuntur, si palam appareant, venditorem non obligant, veluti si dicat servum speciosum, domum bene aedificatam: at si dixerit hominem litteratum vel artificem, praestare debet nam hoc ipso pluris vendit."*

98 Ulp. Dig. 21,1,19,3. *„Ea autem sola dicta sive promissa admittenda sunt, quaecumque sic dicuntur, ut praestentur, non ut iactentur."*

99 Jakab 2013, 187.

physical violence. In addition, of course, we must mention the motive, which is often obvious, that a significant proportion of acts take place under the auspices of economic exploitation. In view of these dogmatic aspects, it is not for nothing that human trafficking is referred to as modern-day slavery. The state of servitude tramples on rights which, through the development of law, have been called fundamental human freedoms. In this context, special mention should be made of the right to life and human dignity; prohibiting torture and inhuman or degrading treatment; the prohibition of servitude and the right to personal liberty and security.

If we wish to draw parallels between the treatment of slaves and the situation of victims of human trafficking today, we can conclude that the past casts quite a shadow over the present. There are many forms of trafficking in human beings that take place in our everyday immediate environment. All of these are based on the abuse of the inherent vulnerability of victims and, as I have already mentioned, are fundamentally based on the exploitation of human beings.[100]

According to the current Hungarian legislation – considering EU and international legal sources[101] – the crime of trafficking in human beings is a complex legal issue, and the legislator punishes it together with forced labour. In line with Article 5 of the Charter of Fundamental Rights of the European Union, Article III of the Fundamental Law of Hungary[102] also contains an absolute prohibition. The Hungarian Criminal Code (Btk.)[103] Section 192, paragraphs 1 and 2,[104] the conduct of the offence can be almost entirely compared to the (part

[100] Report on the implementation of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, point G).

[101] International Convention for the Suppression of the Traffic in Persons and of the Exploitation of the Prostitution of Others, 1950 (New York); Palermo Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children of 2000; Joint Action of 24 February 1997 adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning action to combat trafficking in human beings and sexual exploitation of children; Council Framework Decision of 19 July 2002 on combating trafficking in human beings.

[102] In line with this, see also: The Fundamental Law of Hungary Article II., III., IV., XII., XV.

[103] Act C of 2012.

[104] Section 192 (1) Any person who:
a) sells, purchases, exchanges, or transfers or receives another person as consideration; or
b) transports, harbors, shelters or recruits another person for the purposes referred to in Paragraph a), including transfer of control over such person; is guilty of a felony punishable by imprisonment not exceeding three years.
(2) Any person who - for the purpose of exploitation - sells, purchases, exchanges, supplies, receives, recruits, transports, harbors or shelters another person, including transfer of control over such person, is punishable by imprisonment between one to five years.
(3) The penalty shall be imprisonment between two to eight years if trafficking in human beings is committed:

of) the acts of the ancient Roman slave trade. In view of this aspect, it is not for nothing that human trafficking is referred to as modern-day slavery.

a) against a person held in captivity;
b) by force or by threat of force;
c) by deception;
d) by tormenting the aggrieved party;
e) against a person who is in the care, custody or supervision of or receives medical treatment from, the perpetrator, or if abuse is made of a recognized position of trust, authority or influence over the victim;
f) for the unlawful use of the human body;
g) by a public official, acting in an official capacity;
h) in criminal association with accomplices; or
i) on a commercial scale.
(4) The penalty shall be imprisonment between five to ten years, if:
a) the criminal offense provided for in Subsection (2) is committed against a person under the age of eighteen years;
b) the criminal offense provided for in Subsection (2) is committed against a person held in captivity, and either of the aggravating circumstances under Paragraphs b)-i) of Subsection (3) apply; or
c) the criminal offense provided for in Subsection (2) results in particularly great damage or danger to life.
(5) The penalty shall be imprisonment between five to fifteen years if:
a) the criminal offense provided for in Subsection (2) is committed against a person under the age of fourteen years;
b) the criminal offense provided for in Subsection (2) is committed against a person under the age of eighteen years, and either of the aggravating circumstances under Subsection (3) apply;
c) the criminal offense provided for in Subsection (2) is committed against a person under the age of eighteen years, and results in particularly great damage or danger to life; or d) the criminal offense provided for in Subsection (2) is committed against a person under the age of eighteen years for the purpose of child pornography.
(6) The penalty shall be imprisonment between five to twenty years or life imprisonment if:
a) the criminal offense provided for in Subsection (2) is committed against a person under the age of fourteen years, and either of the aggravating circumstances under Subsection (3) apply;
b) the criminal offense provided for in Subsection (2) is committed against a person under the age of fourteen years, and results in particularly great damage or danger to life; or
c) the criminal offense provided for in Subsection (2) is committed against a person under the age of fourteen years for the purpose of child pornography.
(7) Any person who engages in preparations for trafficking in human beings is guilty of misdemeanor punishable by imprisonment not exceeding two years.
(8) In the application of this Section, 'exploitation' shall mean the abuse of power or of a position of vulnerability for the purpose of taking advantage of the victim forced into or kept in such situation.

The significant difference is, contrary to the legal view of today, that this is a criminalised phenomenon, this form of trafficking was legal in ancient Rome. However, it is worth mentioning again that slaves were considered things and not humans. Based on this conceptual difference, no crime was committed linguistically, but we feel the significant moral malpractice inherent in it.

Bibliography

Géza Alföldy: *Római társadalomtörténet*. Budapest, Osiris, 1996.

Ferenc Bajusz: *Az ókori rabszolgák helyzete és sorsuk alakulása a kereszténység hatása alatt*. Budapest, Budapesti Református Akadémia Kiadó, 1969.

Wayne Edward Boese: *A Study of the Slave Trade and the Sources of Slaves in the Roman Republic and the Early Roman Empire*. Washington, University of Washington, 1973.

Róbert Brósz – Elemér Pólay: *Római jog*. Budapest, Nemzeti Tankönyvkiadó, 1974.

Ágnes Czine: *Az emberkereskedelem, mint a szervezett bűnözés egyik megjelenési formája*. Pécs, s.n., 2011. https://pea.lib.pte.hu/handle/pea/15593.

Ágnes Czine – Andrea Domokos: *Büntetőjog – Különös rész I*. Budapest, Patrocinium Kiadó, 2017.

Andrea Domokos: Az új Büntetőeljárási Kódex sértettekre vonatkozó egyes rendelkezéseiről. *Glossa Iuridica*, 2018/3-4. szám, 137–148.

Andrea Domokos: *Büntető anyagi jog – általános rész*. Budapest, Patrocinium Kiadó, 2019.

Andrea Domokos – Renáta Garai: A bűnözés és a büntető igazságszolgáltatás áldozatai. *Glossa Iuridica*, 2019/3–4. szám, 9–22.

Lenke Fehér: Az emberkereskedelem komplex problémája. *Állam- és Jogtudomány*, 2012/4. szám, 397–420.

András Földi – Gábor Hamza: *A római jog története és institúciói*. Budapest, Nemzeti Tankönyvkiadó, 1996.

Richard Gamauf: *Ad statuam licet confugere*. Frankfurt am Main, Peter Lang GmbH Internationaler Verlag der Wissenschaften, 1999.

István Hahn: Az ókori vallások és a rabszolgaság. *Világosság*, 1965/6. szám, 423–441.

Péter Hahner: *100 történelmi tévhit*. Budapest, Animus Kiadó, 2010.

William V. Harris: Towards a Study of the Roman Slave Trade. *Memoirs of the American Academy in Rome*, 36/1980, 117–140.

Franz Haymann: *Die Haftung des Verkäufers für die Beschaffenheit der Kaufsache I. Studien zum klassischen römischen Recht*. Berlin, s.n., 1912.

Miklós Hollán: Az emberkereskedelem büntetni rendelése a nemzetközi instrumentumok tükrében. *Állam- és Jogtudomány*, 2007/2. szám, 273–287.

Miklós Hollán: Az emberkereskedelem tényállásának jogharmonizációja az európai unióban. *Büntetőjogi Kodifikáció*, 2008/2. szám, 22–26.

Éva Jakab: Rabszolgavételek Rómában. In: Károly Tóth (ed.): *Emlékkönyv Dr. Cséka Ervin születésének 70. és oktatói munkájának 25. évfordulójára*. Szeged, Acta Juridica et Politica, 1992. 247–259.

Éva Jakab: Kereskedési szokások a régi Rómában. *Acta Universitatis Szegediensis: acta iuridica et politica Szeged* XLIV., 1993/7. szám, 9–31.

Éva Jakab: Stipulationes aediliciae (A kellékhibákért való helytállás kialakulása és szabályai a római jogban). *Acta Universitatis Szegediensis: acta juridica et politica Szeged* XLIV., 1993/7. szám, 85–114.

Éva Jakab: *Praedicere und cavere beim Marktkauf. Sachmängel im griechischen und römischen Recht*. München, C. H. Beck Verlag, 1997.

Éva Jakab: *Humanizmus és jogtudomány. Brissonius szerződési formulái I.* Szeged, Pólay Elemér Alapítvány, 2013.

Károly Kubisch: *Az emberkereskedelem büntetőjogi megítélésének morális és szabályozási változásai*. Budapest, s.n., 2021. https://doi.org/10.24395/KRE.2022.005.

Alessandro Launaro: *Peasants and Slaves. The Rural Population of Roman Italy.* Cambridge, Universtity Press, 2011.

Egon Maróti: A délosi rabszolgapiac és a kalózkodás. *Antik Tanulmányok IX.,* 1962/1. szám, 1–12.

Egon Maróti: *Rabszolgák az ókori Rómában*. Budapest, Gondolat Könyvkiadó, 1969.

Ferenc Réthey: *A római rabszolgaság*. Kecskemét, Szél Nándor Nyomda, 1913.

Walter Scheidel: Human Mobility in Roman Italy II. The Slave Population. *The Journal of Roman Studies,* 95/2005, 64–79.

Leonhard Schumacher: Slaves in Roman Society. In: Michael Peachin (ed.): *The Oxford Handbook of Social Relations in the Roman World*. Oxford, Oxford University Press, 2011. 588-608.

Morris Silver: Contractual Slavery in the Roman Economy. *Ancient History Bulletin*, 25/2011, 73–132.

Levente Takács – Dóra Gacsal: A római rabszolgaság. *Korall*, 2016/63. szám, 54–68.

Koenraad Verboven: The Freedman Economy of Roman Italy. In: Sinclair Bell – Teresa Ramsby (ed.): *Free at Last! The impact of freed slaves on the Roman Empire*. London, Bloomsbury Publishing, 2011. 88-109.

Edward Westby: The Roman Slave. *The Law Coach* 3, 1922/5, 76–78.

Szandra Windt: Gondolatok az emberkereskedelemről. *Miskolci Jogi Szemle*, 2019/2. szám, 459–469.

THE REGULATION OF ARTIFICIAL INTELLIGENCE OUTSIDE EUROPE. SECURE AI SYSTEM DEVELOPMENT, GUIDELINES FOR A BETTER FUTURE

Gergely Rideg[1]

ABSZTRAKT ■ A mesterséges intelligencia fejlesztése közkedvelt téma a 21. században. Ez a zabolázatlan technológiai újdonság olyan erővel és letaglózó hatékonysággal érkezett meg a modern gazdasági viszonyok közé, hogy az egyes tényezők hatását igazán még felmérni sem tudják. Egyre gyakrabban jelennek meg újabb és újabb kutatási eredmények azokról a kockázatokról, amelyek a mesterséges intelligencia rendszerek használatával járó különböző kockázatokat elemzik. A jelen tanulmány Nick Bostrom gondolatait is bemutatva és elemezve azokkal a szabályozási problémákkal foglalkozik, amelyek megfejtése a megbízható mesterséges intelligencia rendszerek működtetéséhez nélkülözhetetlen. A tanulmány megteremti a diskurzus alapjait azzal, hogy a kockázat, mint fogalom fundamentumait és határait részletezi, illetve kontextusba hozza és összekapcsolja a mesterséges intelligencia rendszerek kockázataival. Szabályozási kérdéseket vet fel, miközben olyan jó gyakorlatokra és iránymutatásokra hívja fel a figyelmet, mint a „Guidelines for secure AI system development for ensure the secure artificial intelligence development" elnevezésű dokumentum, amely többek között a UK National Cyber Security Centre szervezet részéről került kidolgozásra. A tanulmány olvasásakor betekintést nyerünk a Blueprint for an AI Bill of Rights dokumentumba és felépítésébe, illetve egyéb szakmai iránymutatásokba.

ABSTRACT ■ The development of Artificial Intelligence is a hot topic in the 21st century. This unbridled technological novelty has arrived in the modern economy with such force and staggering efficiency that the impact on individual actors cannot even be truly measured. More and more research are being published on the various risks associated with the use of AI systems. This paper, which also presents and analyses the ideas of Nick Bostrom, addresses the regulatory issues that are essential to the operation of reliable AI systems. The paper lays the foundations for the discourse by detailing the foundations and boundaries of risk as a concept and contextualising and linking the risks of AI systems. It raises regulatory issues, while pointing to good practices and guidelines such as the "Guidelines for secure AI system development to ensure the secure artificial intelligence development", developed

[1] PhD student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

by, among others, the UK National Cyber Security Centre. Reading the paper will provide insights into the Blueprint for an AI Bill of Rights document and its structure, as well as other professional guidelines.

Keywords: artificial intelligence systems, risk analysis, guidelines, cybersecurity, trusted AI, strategies, regulatory problem

1. Introduction

On 13 March 2024, the European Parliament approved a legislation on Artificial Intelligence (AI), which will help the technological innovation of AI while building safeguards to protect our security and fundamental rights.

The European legislator has, in our view, taken a giant step towards taming the technological monster that is now a daily topic of debate around the world.[2]

Why are we looking at regulating the use of artificial intelligence for business purposes? IBM's Global AI Adoption Index 2022 Index[3] found the following: "Today, 35% of companies reported using AI in their business, and an additional 42% reported they are exploring AI. AI adoption is growing steadily, up four points from 2021." In relation to trusted AI, the document highlights the following: "The majority of organizations haven't taken key steps to ensure their AI is trustworthy and responsible, such as reducing bias (74%), tracking performance variations and model drift (68%), and making sure they can explain AI-powered decisions (61%)".

It is clear that companies will pay much more attention to the use of artificial intelligence systems in the future. These technologies will be integrated into their operations. Whose interests will be served by these AI systems and what guarantees do we see?

The focus of the current research is artificial intelligence regulation outside Europe. The research questions are: How is artificial intelligence regulation developing outside the European Union? What are the cornerstones of AI regulation? What are the results, documents, research groups and initiatives that have been carried out so far on the development of artificial intelligence.

[2] Artificial Intelligence Act: MEPs adopt landmark law, https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law (downloaded: 16.03.2024).

[3] IBM Global AI Adoption Index 2022, https://www.ibm.com/watson/resources/ai-adoption (downloaded: 10.02.2024).

The current research is part of a larger research which is now designed to outline the turning points reached by non-European actors.

However, in the following chapters, we will discuss what we consider to be risks and will mention the risks that AI can pose. And through the reflections of Nick Bostrom, we will discuss whether a superintelligence explosion is manageable or problematic.

2. Research method

The research questions will be answered through normative analysis, *interpretatio systematica* and contextual analysis. The analysis will also use an interpretation according to fundamental constitutional rights, as well as an interpretation according to the ethical values behind the law. In articulating the questions, we have kept in mind that the focus is not only on AI as a regulatory subject, but mainly on the role that AI will play/has played in each society, i.e. the social role of AI as a milestone.

3. The historical background of artificial intelligence and the control problem

There are written records from the early days of humankind that humans created fantasy stories about inventing a machine with properties beyond humans. Hephaestus built a bronze structure in the shape of a man, according to mythology. The machine, called Talos, was given by Zeus to King Minos to protect the island of Crete from invaders. The bronze giant, with physical strength beyond human limits, appears in Apollonios Rhodios' Argonautica[4].

Humans create machines so that they can perform an activity faster and more efficiently. Think of the invention of the printer. But in the case of artificial intelligence, there is one more important circumstance. Humanity is building a machine that is smarter and more intelligent than itself. What a paradox follows from this idea, when humans, although they wish to build a machine more intelligent than themselves, do not let its operation out of their hands and wish to exercise their power over that machine by expecting it to operate only according to their will.

[4] Dóra Peszlen: Apollónios Rhodios. Argonautika 3. *Studia Litteraria*, 1-4/2017, 37–41.

It is also important to mention these phenomena because, in the relationship between artificial intelligence and humankind, an important quality or characteristic must be highlighted in order to understand the complexity of the regulatory problem. It relates to the AI-control problem, which Nick Bostrom, Director of the Future of Humanity Institute at Oxford University, describes in his book "Superintelligence: Paths, Dangers, Strategies"[5].

Bostrom puts it bluntly that superintelligence is probably "the most important and greatest challenge humanity has ever faced."

Here, however, we note that what Bostrom is talking about is a superintelligent artificial intelligence, which in his interpretation means a consciousness beyond the smartest human mind. We can take it as a fact that today this kind of artificial intelligence does not exist in this form, and scientists are divided on whether such intelligence could ever exist. Nonetheless, with appropriate abstraction around some of the characteristics of AI and the interpretation of regulatory challenges, Bostrom's thoughts are interesting and useful for the present research questions.

Many experts around the world support Bostrom's claim when they report on the various risks of using artificial intelligence in their analyses. We will not go into a more detailed analysis of the risks of using AI here, but it is necessary to highlight a few ideas in the context of what this paper has to say.

4. The relationship between artificial intelligence and risk

The risk of using AI is a concern for legislators in Europe and beyond. The European legislator has taken explicit steps to identify the scientifically substantiated risks and has started to look for the associated safeguards and guarantees.

On the one hand, the European Commission has identified the benefits of AI in terms of technological improvements for citizens, businesses and public services, such as fewer machine breakdowns, safer transport, better healthcare.[6]

In addition to the benefits, AI also comes with several risks. On the one hand, automatic surveillance, which can be useful, for example for crime prevention purposes[7], can easily lead to a violation of citizens' autonomy. Although the example above also results in a serious violation, people often associate larger scale and more sinister scenarios with irresponsible and financially driven AI

[5] Nick Bostrom: *Superintelligence. Paths, Dangers, Strategies*. Oxford University Press, 2014.

[6] COM(2020) 65 final 2.

[7] In Mannheim, an automated system reports hugs to the police, https://algorithmwatch.org/en/mannheim-system-reports-hugs-police/ (16.02.2024).

development.[8] The science fiction literature and film industry played no small part in this. Autonomous weapon systems that cause death are often mentioned in this context. The development of these is currently shrouded in obscurity, but a large part of the international legal community is strongly in favour of a prior ban on such weapons. An example of such a ban is the 1995 ban on the use of laser weapons that cause permanent blindness.[9] Autonomous weapons systems, also known as killer robots, raise serious ethical concerns and could be a catalyst for a dangerous arms race. The number of potential victims is yet scientifically incalculable, which is why it is a fact that they pose immense risks at the level of society as a whole.

What do we mean when we say that using artificial intelligence is risky? What do we mean by risk? Nowadays, almost every day, everyone can see the use of artificial intelligence on the front pages of the press in various areas of our daily lives. From the artificial intelligence solutions in medicine[10] to the facial recognition applications lurking on our mobile phones, we see artificial intelligence analysing millions or billions of personal data almost every hour. What everyone probably already knows is that artificial intelligence is a risky entity. However, there is concern that society is only aware of this assumption about AI and that it is not being looked at with a sufficiently complex vision.

The risk of AI has been mentioned above, but we have not addressed what exactly we mean by risk. In the following, I will make some basic observations in this context, which will be used to assess the results of the European entities in the following chapters.

According to general risk theory, risk is obtained by considering (multiplying) two factors, the probability of a negative event occurring on the one hand, and the magnitude of the negative consequences of the event on the other hand.[11]

[8] Ethical Guidelines for Trusted Artificial Intelligence prepared by the High Level Expert Group on Artificial Intelligence.

[9] Protocol on Blinding Laser Weapons, https://fas.org/nuke/control/ccw/text/protocol4.htm (downloaded: 17.11.2020).

[10] In recent years, there has been considerable research into the use of AI in the medical field. According to a study published in the Journal of the American Medical Association, AI-based systems can, among other things, accurately diagnose common skin conditions with an accuracy comparable to that of human dermatologists. Another study published in the journal Nature showed that AI can analyse genetic data and identify personalised treatment options for patients with rare diseases.

[11] József Kindler: Általános kockázatelmélet és -módszertan. Egyetemi jegyzet. 1983. cited by Tamás Fleischer: Innováció, növekedés, kockázat. In: Miklós Bulla – Pál Tamás (eds.): *Fenntartható fejlődés Magyarországon. Jövőképek és forgatókönyvek.* Budapest, Új Mandátum Könyvkiadó, 2006. 275-284. http://real.mtak.hu/3973/1/fleischer_innovacio-novekedes-kockazat_fefemao06.pdf (01.03.2021).

Also, different disciplines have different interpretations of risk.[12] In economics, for example, loss is accompanied by the optional occurrence of gain. In general, however, it is associated with the possibility of danger, injury, damage or death. From the above equation, it can be deduced that both higher frequency and more severe consequences lead to an increase in risk. There are different classifications of risk, so we can and should distinguish between, for example, individual and global risk, direct and latent, controllable and uncontrollable, voluntary and involuntary, subjective and objective risk, etc. Objective risk, which is more relevant to our topic, is estimated based on a large number of repeated experiments, while subjective risk estimates are based on a small number of observations or possibly on conjecture. In between the above two is synthetic probability, where the probability of an event occurring is not measured directly but modelled. In modelling, the event is estimated based on similar objective probability systems.[13]

However, we also see that people tend to base their expectations and decisions on subjective estimates of risk, so there is a large discrepancy between social perception and the outcome of a scientific, empirically measured probability estimate,[14] which in turn determines their confidence in the risky thing. This concept leads us to the regulatory side of risk analysis and risk assessment.

Trust is key to the regulation of artificial intelligence, as András Tóth argues in relation to the paradox of regulating artificial intelligence; to fulfil the purpose of AI for the benefit of people, trust must be instilled in the technology.[15] Guarantees must be built into the legislation that is being developed to ensure human rights and ethical principles in AI applications. The regulation must therefore build in safeguards to ensure that when AI is used to serve people, it does not violate fundamental human rights, it is transparent in its operation and the decision-making process can be monitored. For example, the autonomous heavy machinery installed in the Mohács iron foundry should not be able to harm its operators in the event of a malfunction.

When identifying the risks posed by AI applications, it is therefore appropriate to use objective estimates, which should be based on many repetitive cases identified as a result of scientific studies (precaution principle).

The context of the analysis is defined by our view – in agreement with Ulrich Beck's ideas on the subject – that in the 21st century we live in a risk society.

[12] Fedja Netjasov – Janic Milan: A review of research on risk and safety modelling in civil aviation. *Journal of Air Transport Management*, 4/2008, 213–220.

[13] Ádám Havas: Kockázatelemzés-mágia vagy tudomány? *Iskolakultúra*, 23/1993, 21–28.

[14] Fleischer 2006.

[15] András Tóth: A mesterséges intelligencia szabályozásának paradoxonja és egyes jogi vonatkozásainak alapvető kérdései. *Infokkumunikáció és jog*, 73/2019, 3–9.

Advanced industrial society is itself an extractor of social risks, and "differences in education, skills, access to information and income determine the risk burden of different social groups".[16]

In the context of the above, Bostrom's book[17], in which he analyses the dynamics of the explosion of super intelligence that does not yet exist, contains some very exciting ideas. It looks at what happens once this intelligence is in place, and how we can create the initial conditions to drive this particular explosion towards positive outcomes.

Among many other factors, Bostrom sees the risk of AI in the agent principal problem as follows. He poses the question, "how can the sponsor or promoter of a project to develop superintelligence ensure that the superintelligence created by a successful project will serve the sponsor's goals?" Putting the question in a slightly more common law context, we think of a company whose owners wish to create an artificial intelligence system with a particular function, for which they set out the ethical, moral, economic, and functional guidelines they consider important. How can they be sure that the system they create will meet all their guidelines? The owners entrust the company's chief executive officer (agent) with the task. The principal-agent problem, well known to economists, is encountered. This is an important case of incomplete information games. Here, the following factors are at play: an agent has choices; he is expected to make decisions in the best interests of the principal; but the principal cannot observe the choices he makes, the choices he has made, the alternatives he has chosen, or whether he has chosen the best choice.[18] The agent can make good decisions and bad decisions. It can be a bad result in the light of the fact that the agent has otherwise made good decisions. By bad decisions we mean when he has made a decision because, as a trustee, he does not bear the consequences of his decision, because if he had, he would have made a different decision. Of course, we can take security measures to ensure that the principal carries out the task entrusted to him in the most favourable way for the principal. But this obviously comes at a price. It is a question of cost-effectiveness. The project owner must consider what resources he can allocate to motivate the agent, the software developers, to make the desired decisions. It may also decide to introduce more stringent controls or a stricter screening of developers.[19] In these cases, however, the potential damage to the risk side of AI systems must always be considered.

16 Fleischer 2006, 279.

17 Bostrom 2014.

18 Ákos Szalai: *Közgazdaságtani fogalmak és módszerek jogászoknak*. Budapest, Pázmány Press, 2020. 117-118. https://mek.oszk.hu/21800/21884/21884.pdf (13.03.2024).

19 Bostrom 2014, 188.

On the legal side, questions will arise as to whether the project owner has taken all reasonable measures to mitigate or manage the known risks.

Bostrom breaks down the above agent problem in the development of artificial intelligence into two cases. One is the first problem mentioned above, where the agent and the developer are both humans. Then, in his view, the problem mainly arises in the development phase. The author also predicts that in this case the usual management techniques can be applied to deal with the problem. It is pointed out, however, that the characteristics of artificial intelligence should be considered to a greater extent in the specific development methodology. Without going into a detailed analysis of the techniques, as this is beyond the scope of this research, we believe that the application of management techniques alone is not a sufficient guarantee.

In the other case, the principal and the agent are the superintelligence. He believes that this is a problem at the operational stage. To solve this problem, new techniques are needed.

The paper analyses the problems of managing artificial intelligence as follows.

He sees the methods for managing the potential explosion as falling into two broad categories. On the one hand, we can talk about the control of capabilities, and on the other hand, the selection of motivations. With the former, we can place limits on the scope of the AI, and with the latter, we can control what it strives to do. The first of the capability control methods to be mentioned is the box method, which is reminiscent of the 'sandbox" methods that are prevalent in AI research today.[20] In this method, we distinguish between physical and informational restriction methods. And the essence is nothing other than to lock in artificial intelligence. In this situation, an attempt is made to prevent the AI from interacting with the outside world outside the channels provided by the researchers. The method of restricting information from the outside works by trying to control what information can enter the box.

Among the methods used to regulate ability are restraint, incentives and traps. Traps, as a mechanism, work by having a mechanism independent of the AI run diagnostic tests on the system itself and stop it if it detects dangerous threat signals. This method may be suitable for use as a temporary safeguard during the development phase.

Among the methods of motivation selection, Bostrom mentions direct specification first. This method brings us to the main problem for lawyers. How do we regulate artificial intelligence systems? Motivation selection methods seek to shape the will of the superintelligence. In this way, we might be able to

[20] AI Sandbox, https://huit.harvard.edu/ai-sandbox 20.03.2024).

prevent unwanted outcomes. We then seek to control the system's motivations and ultimate goals. The direct specification tries to define the artificial intelligence in a rule-based and consequence-based way using some rules or values. In the book, we find examples of how machines can be induced to follow Asimov's laws or to obey the rules of different countries' legal systems. The main problem is that in all cases the rules must be precise, applicable in all situations and translatable into machine language. It is also difficult to determine what to assign value to, or even how to define a concept.

To add to Bostrom's thoughts, we would like to nuance the problem and draw attention to the complexity of the issue in the following. We also run into a hurdle in defining the principles used to regulate artificial intelligence when we consider that each statement is a matter of relativity. In fact, if we want to specify that the AI system should take care of environmental sustainability and, in this context, water quality adequacy, that it should focus on adequate water quality, and we plant this as a kind of principle in its codes, we are faced with the following problem. When considering the derived value of 'water quality' for environmental sustainability, we find two contradictory criteria. Here, the "quality of drinking water" and the "quality of the food chain of fish populations" are in conflict. The comparison is based on whether we are part of the population using the lake as a drinking water reservoir or whether we are anglers or conservationists, for whom the latter factor is more important. The right 'phosphate level' is cardinal, as lower phosphate levels are better for drinking water quality but worse for fish populations."[21] Therefore, to make a proper assessment, we need to determine the case-by-case order of the values.

Bostrom's book concludes with the question of what we should do to properly manage the explosion of super intelligence. As well as drawing attention to the need to assess our strategic situation and build capacity, he points to the need to take specific measures. He mentions developments in the field of technical problems of machine intelligence security as just such a specific measure. It also has a specific objective to help spread "good practices" among AI researchers. He believes that any progress on the problem of governance should be communicated to all researchers.

A series of good practice documents have been published around the world in recent years. Various organisations have set out ethical and moral lines and frameworks[22] for the safe and trustworthy use of AI in specific industry sectors.

[21] From Principles to Practice, An interdisciplinary framework, https://www.ai-ethics-impact.org/resource/blob/1961130/c6db9894ee73aefa489d6249f5ee2b9f/aieig---report---download-hb-data.pdf 17. (26.11.2022).

[22] UNESCO Recommendations on the Ethics of AI, November 2021. or UNICEF Policy Guidance on AI for Children, November 2021.

One such guideline will be described in detail below, followed by a document containing similar good practices and guidelines.

5. Guidelines for secure AI system development to ensure the secure artificial intelligence development

The timeliness of regulating artificial intelligence (AI) is beyond debate. In addition to the opportunities offered by new technologies, there is now a detailed mapping of the risks surrounding AI systems.

Highly advanced AI is predicted by prominent figures from different disciplines as a technology with gigantic risks.[23] Risk factors are linked to a broad spectrum of fundamental human rights, highlighting the potential dangers of using AI.[24]

On 11/27/2023, artificial intelligence regulation reached another milestone. On this day, the National Security Agency (NSA), UK National Cyber Security Centre (NCSC-UK), U.S Cybersecurity and Infrastructure Security Agency (CISA) and other partners released their global guidelines, which are guidelines for secure AI system development to ensure secure artificial intelligence development.

23 partners from 18 countries have joined the document and agencies from all corners of the globe have contributed to the document from Chile to France and Japan. This reflects the cross-national challenges of AI systems from a cybersecurity perspective.

Of course, this document is not without precedent, as the National Cyber Security Centre previously published another document[25] in August 2022, entitled "Principles for the security of machine learning", which also addressed fundamental principles to address and prevent the additional risks inherent in machine learning systems.

As digitalisation becomes more and more prevalent in our lives and we spend more and more time online, the security of these technologies becomes crucial. Besides expecting IT hardware to be secure, it is equally important that software provides the right level of security. Public administrations, among others, are

[23] Around April 2023, it was reported in various media that decisive people such as Elon Musk, Yuval Noah Harari and Steve Wozniak, among others, are calling for an immediate halt to the development of certain types of artificial intelligence systems. Die Rückkehr des Wunderglaubens, https://www.spiegel.de/wissenschaft/kuenstliche-intelligenz-die-rueckkehr-des-wunderglaubens-kolumne-a-d53eb350-b5b5-4888-9bf8-8fc510d018b8 (15.04.2023).

[24] Sándor Udvary: Az önvezető gépjárművek egyes felelősségi kérdései. *Pro Publico Bono – Magyar Közigazgatás,* 2/2019, 146–155.

[25] Principles for the security of machine learning, https://www.ncsc.gov.uk/files/Principles-for-the-security-of-machine-learning.pdf (10.09.2023).

also trying to get on board this digitalisation trend and many services are now available either optionally or exclusively in digital form. There is no doubt that serious problems can arise when some public services become dysfunctional, for example when they stop working, as a result of cyber-attacks. Failures in software and hardware products increase the attack surface on which cybercriminals can cause damage.

The importance of these guidelines is also underlined by the fact that several non-governmental organisations have contributed to their development. It is encouraging to note that the list includes several major global IT companies such as Google, Microsoft, Amazon, IBM, etc., which are playing a key role in the digital development process.

Tech giants such as Microsoft, which are pioneers in the development of various AI systems at many points – think of their partnership with OpenAI – naturally have their own AI security protocols. [26] In the document "AI security risk assessment framework", published on 9 December 2021, they explicitly address machine learning security assessment, within which they specifically address the secure storage, access and integrity of the data used, the types of sensitive data and they elaborate on the security criteria for models. It includes professional guidelines such as that the source of the data collected should be verified before use, the source should be stored with the data and documented. In addition to these, it is also more specific in its cultivation and includes criteria specifically for model teaching and development.[27]

Looking more closely at the NCSC published guidelines document we discuss, we see that, as in the Microsoft document, artificial intelligence is specifically defined as machine learning applications, and within that, all types of machine learning AI are included. In line with the technological developments and trends of the time, AI systems are typically based on machine learning models.

To be clear from an application perspective, the document also provides a definition of machine learning applications. "MI applications are applications that:

- involve software components (models) that allow computers to recognise and bring context to patterns in data without the rules having to be explicitly programmed by a human
- generate predictions, recommendations, or decisions based on statistical reasoning."

[26] Best practices for AI security risk management, https://www.microsoft.com/en-us/security/blog/2021/12/09/best-practices-for-ai-security-risk-management/ (10.09.2023).

[27] Microsoft Security AI Security Risk Assessment, Best practices and guidance to secure AI systems,https://github.com/Azure/AI-Security-Risk-Assessment/blob/main/AI_Risk_Assessment_v4.1.4.pdf (10.09.2023).

As to the reasons for the creation of this document, the document declares the following. Just like in other areas of our lives, new tools and new techniques in programme development provide opportunities for new abuses. Before the advent of car use, it was not natural for an accident to be caused by deliberately damaging parts of a car. Artificial intelligence systems contain new vulnerabilities that can be exploited by prepared malicious actors, both on the hardware and software side. The paper draws attention to this by stressing that attackers can induce unintended behaviour in machine learning systems by using so-called adversarial machine learning, leading to the problem repeatedly mentioned by lawyers that the output of the system cannot be predicted. In the case of machine learning AI systems, this "black box effect" is present anyway, in the case of such cyber-attacks this unintended behaviour is deliberately induced.

There can also be cases where users are allowed to perform unauthorised operations, or data poisoning, where the training data as a data domain is corrupted.

The structure of the document follows the 4 phases in the lifecycle of AI systems development, namely secure design, secure development, secure deployment, and secure operation and maintenance.

This life cycle includes the requirement that once the software containing the AI systems is created, it is monitored during its use, with each update meeting cybersecurity criteria.

In fact, in each chapter, the document suggests considerations and measures that will help reduce the overall risk of the organisational AI system development process.

One such suggestion is to consider the security benefits and trade-offs of each model when selecting an AI model at the design stage of development.

By integrating well-established principles like "security-by-design" and "security-by-default", the publication outlines the existing vulnerabilities specific to AI and suggests ways to consider them during the development process. Typically, end users lack the understanding to grasp the risks associated with AI. Additionally, cybersecurity authorities emphasize the importance for AI system operators to educate users about potential risks and provide guidance on the secure utilization of these systems.[28]

While the document certainly describes the guidelines in sufficient detail for its intended purpose, the agencies emphasize that the measures and adherence to such guidelines are not a substitute for the development of a proper cybersecurity practice and risk management program or protocol. Such research itself should

[28] Internationale Cybersicherheitsbehörden veröffentlichen Leitfaden zur Entwicklung sicherer KI-Systeme, https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2023/231127_Leitfaden-sicher-KI-Systeme.html (13.01.2024).

be used in conjunction with established cybersecurity risk management and incident response best practices. The guidelines set out in this document are closely aligned with the good practices for software development lifecycle practices that have already been identified in subsequent documents:

- the NCSC's Secure development and deployment guidance
- the National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF)6

The document is not binding legislation that would impose a strict obligation on companies developing AI systems, and thus cannot be used to enforce its provisions. However, it is noted that the use of new technologies and the success of AI systems are based on trust and confidence in them, which cannot be achieved by legislation alone. This document can be successful and can be considered a milestone because of the significant international partnership and contributors.

Increasing user awareness creates the need for the system to be used to comply with cybersecurity recommendations. This kind of user confidence can be achieved by applying a standard, by obtaining a certificate, with which an operator can not only be successful, but also help build a more secure digital future for its users.

6. Blueprint for an AI Bill of Rights

In late 2022, the White House proposed a Blueprint for an AI Bill of Rights. "The Blueprint for an AI Bill of Rights is a set of five principles and associated practices to help guide the design, use, and deployment of automated systems to protect the rights of the American public in the age of artificial intelligence."[29] The five principles are the followings: safe and effective systems; algorithmic discrimination protections; data privacy; notice and explanation; human alternatives, consideration, and fallback.

The document provides concrete guidance on the principles to be applied to address the identified risks, which can provide appropriate safeguards to ensure that the design, development and operation of AI systems do not cause any harm. The document stresses that it has been drawn up following appropriate public consultation and that the conclusions drawn therefrom are included.

[29] Blueprint for an AI Bill of Rights, https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf (22.12.2023).

This framework provides a national values statement and toolkit that is sector-agnostic to inform building these protections into policy, practice, or the technological design process.

The document also integrates itself into the legal order by expressing that "where existing law or policy – such as sector-specific privacy laws and oversight requirements – do not already provide guidance, the Blueprint for an AI Bill of Rights should be used to inform policy decisions."

What makes the document unique is that, in addition to the general principles, it provides the reader with concrete guidance and a toolbox by answering the following questions for each principle. Why is this principle important? What should be expected from automated systems? How can these principles move into practice? These are the questions that market players who want to prepare for the use of AI are also asking about the practical application of AI and risk management. However, let's see how far this document really succeeds in answering these questions by means of a concrete example.

In our opinion one of the most interesting principles is the "human alternatives, consideration, and fallback".

We find this important and interesting because the system is designed to bypass humans to perform a task faster and more efficiently. On the other hand, it is also linked to the realisation that we know the exponential nature of artificial intelligence and, as mentioned earlier, its ability to cause enormous damage in a very short time. For this reason, the document stresses that "you should be able to opt out from automated systems in favour of a human alternative, where appropriate."

In response to the question why this principle is important, the document details the following:

"No matter how rigorously an automated system is tested, there will always be situations for which the system fails."

This principle is essentially nothing more than a so-called "kill switch"[30], which serves the purpose in the IT sector of switching off a program or device if it starts to malfunction. This is not only necessary when using artificial intelligence systems, it should be part of any program that may malfunction. However, this technique is, by definition, a system in operation and not a preventive technique. It makes sense to talk about guarantees built in and applied during the development of the programme and guarantees during the operation of the programme, both for AI systems and for other IT solutions. The principle under analysis here

[30] Will There Be A 'Kill Switch' For AI?, https://www.forbes.com/sites/cognitiveworld/2020/03/05/will-there-be-a-kill-switch-for-ai/ (12.01.2024.).

focuses on the monitoring of the program once it is running. The amount of damage that occurs in this case depends on when the human supervisor detects the error and the time that elapses between the detection of the error and the pressing of the *off* button.

It also uses negative examples to illustrate the damage that can occur if the principle is ignored. In a Colorado unemployment benefit scheme, claimants were required to have a smartphone to prove their identity. Understandably, those who did not have a mobile phone could not identify themselves due to a lack of human means.

After identifying, why the principle is important for the community, the document also gives examples of how the principle can be put into practice. Examples include systems to help employees choose the right health insurance for their needs in the marketplace, and customer service systems to help answer common problems and questions. Perhaps a shortcoming of the document is that these examples are not very detailed and numerous. Nevertheless, they are properly referenced so that specific cases that have occurred can be traced.

7. Other examples of good practice

While the Blueprint may be a milestone in terms of good practice, we nevertheless believe that there are more sophisticated and useful documents for users who are new to AI.

Such documents have been produced under the auspices of the OECD. One of these is "The state of implementation of the OECD AI principles four years on"[31] which shares with the reader in a detailed way the practices of implementing the principles promoted by the OECD. It gives the quality seal created by the German AI Association to promote the use of human-centred and human-serving AI as an example. This seal identifies a common set of values and validation processes to express the ethical compatibility of products. The key criteria are ethics, impartiality, transparency, security and privacy.

31 The state of implementation of the OECD AI Principles four years on, https://www.oecd-ilibrary.org/docserver/835641c9-en.pdf?expires=1712094731&id=id&accname=guest&checksum=65B325A7C953BC3F 7BE8B89128BE9F6E (12.01.2024.).

Documents[32] and webpages[33] published by Ernst & Young Global Limited showcase the potential of AI for business through real-world, authentic examples.

The document "The Artificial Intelligence (AI) global regulatory landscape" has the great advantage of outlining regulatory trends, but also provides recommendations on what steps individual companies and policy vendors can take to ensure the safe use of AI.

We find examples for leading practices to create a trusted AI ecosystem. It is necessary to have Al ethical design policies and standards for the development of Al, including an Al ethical code of conduct and Al design principles. The Al ethical design standards should define and govern the Al governance and accountability mechanisms to safeguard users, follow social norms and comply with laws and regulations.

There is a need for related strategies, so that artificial intelligence and its control develop in the right direction.

Regulating artificial intelligence is very important, according to which various non-European countries included their artificial intelligence strategies, which they formulated, starting in 2017. These strategies outline the main regulatory directions and ethical directives around which the regulation is intended to be built. Without analyzing these strategies in more detail, we note that, for example, in March 2017 Canada published the Pan-Canadian Artificial Intelligence Strategy. South Korea also published its Artificial Intelligence Strategy for Innovative Growth in December 2018.

Country	**Name of the document**	**Date of issue**
United States:	Executive Order on Maintaining American Leadership in Artificial Intelligence	February 2019
Canada	Pan-Canadian Artificial Intelligence Strategy	March 2017
China	New Generation Artificial Intelligence Development Plan	July 2017
South Korea	Artificial Intelligence Strategy for Innovative Growth	December 2018
United Arab Emirates (UAE)	National AI Strategy	October 2017,
India	National Strategy for Artificial Intelligence	June 2018
Russia	National Strategy for AI	October 2019
Saudi Arabia	SDAIA Strategy	August 2019

[32] The Artificial Intelligence (AI) global regulatory landscape, https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/ai/ey-the-artificial-intelligence-ai-global-regulatory-landscape.pdf (20.02.2024).

[33] AI Use cases, https://www.ey.com/en_gl/services/ai/use-cases#tabs-ca1ee0a390-item-1c236c7145-tab (28.01.2024).

8. Conclusion

Summarizing the above, we can see that there is no lack of theoretical foundations, ethical guidelines and researched philosophical arguments regarding the development of artificial intelligence. Research on the regulation of artificial intelligence is a very popular field in twenty-first century law and engineering. The question arises, then, what is the obstacle to the regulation of AI and the kind of positive intelligence explosion that Nick Bostrom has predicted.

In our view, the common intelligence, the kind of subjective risk measurement discussed in the previous chapters and the development of all these are the goal to put this technological progress into operation.

We have seen examples of good practices that can help companies to implement AI applications safely. Some of the papers point to the important role that standards will play in promoting good technical documentation. The relevance and usefulness of good practices will be seen over time, and time-proven good practices will certainly contribute to the low-risk operation of AI systems. As pointed out in the Ernst & Young paper cited above in relation to existing regulatory trends, regulators are seeking to link AI guarantees with other areas such as data protection. In this respect, we believe that it will be important in the future not only to understand how AI works, but also to successfully link the regulation of AI with existing regulation and different regulatory areas. In this context, it is essential to understand the nature of artificial intelligence and the risks of artificial intelligence systems. It is important to stress that this task requires staff with multidisciplinary knowledge, as is the case in this area.

We think it is important to underline our view that, although good practices in a market context can certainly prove useful, as the consumer will choose a higher quality and safer product, the truly reassuring thing would be the regulation of artificial intelligence that can be embedded and enforced in the relevant legal system. That is why we welcome the efforts of the European legislator in this direction.

Bibliography

Ádám Havas: Kockázatelemzés-mágia vagy tudomány? *Iskolakultúra*, 23/1993, 21–28.

András Tóth: A mesterséges intelligencia szabályozásának paradoxonja és egyes jogi vonatkozásainak alapvető kérdései. *Infokkumunikáció és jog*, 73/2019, 3–9.

Artificial Intelligence Act: MEPs adopt landmark law, https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law (downloaded: 16.03.2024)

Blueprint for an AI Bill of Rights, https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf (22.12.2023)

Dóra Peszlen: Apollónios Rhodios. Argonautika 3. *Studia Litteraria*, 1-4/2017, 37–41.

Fedja Netjasov – Janic Milan: A review of research on risk and safety modelling in civil aviation. *Journal of Air Transport Management*, 4/2008, 213–220.

IBM Global AI Adoption Index 2022, https://www.ibm.com/watson/resources/ai-adoption (downloaded: 10.02.2024)

József Kindler: *Általános kockázatelmélet és -módszertan. Egyetemi jegyzet*. 1983.

Nick Bostrom: *Superintelligence. Paths, Dangers, Strategies*. Oxford University Press, 2014.

Ákos Szalai: *Közgazdaságtani fogalmak és módszerek jogászoknak*. Budapest, Pázmány Press, 2020. https://mek.oszk.hu/21800/21884/21884.pdf (13.03.2024)

Tamás Fleischer: Innováció, növekedés, kockázat. In: Miklós Bulla – Pál Tamás (eds.): *Fenntartható fejlődés Magyarországon. Jövőképek és forgatókönyvek.* Budapest, Új Mandátum Könyvkiadó, 2006. 275-284. http://real.mtak.hu/3973/1/fleischer_innovacio-novekedes-kockazat_fefemao06.pdf (01.03.2021)

A folyóirat a Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskolájának a közleménye. A szerkesztőség célja, hogy fiatal kutatók számára színvonalas tanulmányaik megjelentetése céljából méltó fórumot biztosítson.

A folyóirat közlésre befogad tanulmányokat hazai és külföldi szerzőktől – magyar, angol és német nyelven. A tudományos tanulmányok mellett kritikus, önálló véleményeket is tartalmazó könyvismertetések és beszámolók is helyet kapnak a lapban. A beérkezett tanulmányokat két bíráló lektorálja szakmailag. Az idegen nyelvű tanulmányokat anyanyelvi lektor is javítja, nyelvtani és stilisztikai szempontból. A folyóirat online verziója szabadon letölthető (open access):
https://ajk.kre.hu/index.php/kiadvanyok/studia-iuris.html

3790 Ft
ISSN 3057-9058
9 773057 905048