ISSN 2949-2483

Volume 1 Number 4

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2023

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

Volume 1, № 4
2023

DOI: 10.21202/2949-2483.2023.4

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

eISSN 2949-2483

Published since 2023, frequency – 4 issues a year. DOI: 10.21202/2949-2483

Editorial Board

Editorial

Address: 42 Moskovskaya Str., 420111 Kazan, Russian Federation
Tel.: +7 (843) 231-92-90
Fax: +7 (843) 292-61-59
E-mail: lawjournal@ieml.ru
Website: https://www.lawjournal.digital
Telegram: https://t.me/JournalDTL_world
VKontakte: https://vk.com/JournalDTL
Yandex.Dzen: https://dzen.ru/JournalDTL
Odnoklassniki: https://ok.ru/JournalDTL

Founder and publisher of the Journal

Kazan Innovative University named after V. G. Timiryasov. Address: 42 Moskovskaya Str., 420111 Kazan, Russian Federation. Tel.: +7 (843) 231-92-90. Fax: +7 (843) 292-61-59. E-mail: info@ieml.ru. Website: https://ieml.ru

Date of signing the issue for publication: 2023, November 30. Hosted on the website https://www.lawjournal.digital: 2023, Desember15.

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Том 1, № 4
2023
DOI: 10.21202/2949-2483.2023.4
ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL
eISSN 2949-2483

Content

Research article
DOI: https://doi.org/10.21202/jdtl.2023.37

Digital Inclusion for People with Autism Spectrum Disorders: Review of the Current Legal Models and Doctrinal Concepts

James Hutson
Lindenwood University
Saint Charles, United States

Piper Hutson
Lindenwood University
Saint Charles, United States

Keywords

autism,
accessible environment,
legislation,
disability,
law,
autism spectrum disorder,
social security,
digital accessibility,
digital inclusion,
digital technologies

Abstract

Objective: today, a significant part of professional tasks are performed in the digital environment, on digital platforms, in virtual and other meetings. This necessitates a critical reflection of traditional views on the problem of accessible environment and digital accessibility, taking into account the basic universal needs of persons with disabilities.

Methods: a gap between the traditional legal perspective on special working conditions for persons with disabilities and the urgent need of a digital workplace (digital environment) clearly shows lacunas in the understanding of accessibility, which are identified and explored with formal-legal and doctrinal methods. The multifaceted aspects of digital inclusion are revealed based on an informative approach to legislation. It leads, among other things, to searching for recommendations which would fill this gap and contribute to the creation of a more inclusive and responsible legal, social and technological environment.

✉ Corresponding author

Results: the research has led to a conclusion that the existing legal, social and technological paradigms need to be re-evaluated. This reevaluation should aim to develop a more inclusive and benevolent concept of accessible environment that takes into account the diversity of human experience and needs, and a wide range of behavioral and cognitive characteristics. Creating special conditions in the workplace for those with overt and covert health problems should become an integral part of the employer's focus, along with improving management efficiency.

Scientific novelty: covert (hidden) health problems have traditionally been understudied, although they include a range of mental and physical impairments, which, like explicit health problems, vary in their origin, intensity, and permanent or episodic character. This study fills a gap in the issues of disability and its legal protection, taking into account the trend of digital inclusion, the dynamic labor activity of today, and the wide range of human abilities and needs.

Practical significance: the aspects of hidden or latent disability considered in the study provide a different perspective at employment, focusing on the workplace conditions that could be created. Employers may be unaware of the need to create special working conditions for those with hidden health problems. This results in negative effects on unemployment, increased sick leave, limited opportunities in the workplace, and more. Employees are often reluctant to disclose their non-obvious health problems to employers; hence, employers should facilitate disclosure of such information by creating relevant conditions. Such an approach will contribute to the legal protection of this category of employees and to further development of the existing legislative regulation, since the latter does not fully comply with today's needs and changed reality.

For citation

Hutson, J., & Hutson, P. (2023). Digital Inclusion for People with Autism Spectrum Disorders: Review of the Current Legal Models and Doctrinal Concepts. *Journal of Digital Technologies and Law, 1*(4), 851–879. https://doi.org/10.21202/jdtl.2023.37

Contents

Introduction

Invisible disabilities encompass a spectrum of mental and physical impairments that, akin to observable disabilities, diverge in their origin, intensity, and permanence or episodic nature. Concerning disability in the workplace, the argument is advanced that absent from the discourse are individuals with one of the most concealed disabilities—specifically, individuals with autism—and the corresponding legal obligations (Neely & Hunter, 2014). Past international research efforts in Canada have posited that invisible impairments may be present in as many as 40% of individuals with disabilities (Matthews & Harrington, 2000). Furthermore, the subject of invisible disability warrants attention due to its disputed status as both a valid condition and diagnosis, with implications extending into the spheres of individual existence, cultural attitudes, public policies, and occupational practices. Reeve & Gottselig (2011) observed, "Because invisible disabilities have traditionally not received the recognition that other forms of disability have, employers may not be aware of the need to accommodate people with invisible disabilities. Lack of accommodation results in lower employment rates, increased work-related absences and a restriction of capabilities within the workplace, among other things." The concealed or latent aspect of disability offers a lens through which the matter of employment may be explored, with particular emphasis on the accommodations that might be devised within the labor market's workplaces.

Furthermore, there is a conspicuous absence in much of the conventional literature concerning employment and disability in an examination of decisions to disclose a concealed disability on the part of the employee to an employer. Disclosure, although a pathway to workplace accommodation and potentially beneficial for the employee with a disability, remains fraught with risks, carrying both potential advantages and disadvantages. The resultant scenario forms a dilemma concerning disclosure for employees with invisible disabilities (Prince, 2017). The onus is on employers to foster a workplace environment that encourages the disclosure of invisible disabilities. This can be achieved through clarity in delineating the competencies requisite for a role, providing comprehensive information in accessible formats beforehand, and permitting opportunities for disclosure throughout the recruitment and selection procedures. Accommodation in the workplace for individuals with visible or invisible disabilities often transcend mere exceptions. Rather, the focus is on effective management, characterized by explicit expectations, transparent communication, and inclusive practices. Such an approach is in line with legal protections afforded this population of workers (Patton, 2022).

A segment of the population that has been notably overlooked in the discourse surrounding invisible disabilities pertains to individuals associated with Autism Spectrum Conditions (ASC). While legislative and societal advancements have been made in addressing certain disabilities, the complex and multifaceted needs of those with ASC are frequently marginalized. Autism, by its nature, defies generalization, encompassing a wide range of behavioral and cognitive traits that can vary significantly among individuals. The subtle and often misunderstood manifestations of ASC may lead to misconceptions

and a lack of tailored support in both the workplace and broader societal contexts. Current legal frameworks, such as the Americans with Disabilities Act (ADA), have shown limitations in addressing these specific and nuanced needs. The failure to adequately recognize and support individuals with ASC is indicative of a broader systemic flaw, wherein legal, societal, and technological paradigms fail to fully comprehend and cater to a diverse spectrum of neurodivergent experiences. Therefore, there exists an urgent necessity to expand the prevailing understanding of accessibility beyond traditional perspectives, to create an environment that is genuinely inclusive and responsive to the real-world complexities associated with ASC.

The present study endeavors to both challenge and enrich prevailing viewpoints concerning accessibility, with a central argument positing that what are often referred to as «special» or «disabled» needs are fundamentally human and universal. While recognizing the significant progress made by the Americans with Disabilities Act (ADA) in delineating guidelines for physical accessibility and accommodations for visual impairments, the research highlights a conspicuous deficiency in addressing the multifaceted requirements of neurodivergent populations. This deficiency extends to individuals with conditions such as dyslexia and color blindness. The current tendency to label these needs as «special» emerges as a concerning phenomenon within the discourse, one that risks unintentional marginalization and relegation to a secondary status. In addition, the study undertakes a critical examination of the hiring practices of accessibility officers within the domains of technology and UI/UX. Current recruitment strategies, the study finds, are frequently narrowed to specific considerations, such as low-vision readability, thereby neglecting a broader spectrum of neurodivergent accessibility that encompasses information processing and cognitive overload. This lacuna points to a disconcerting disconnect between existing legal statutes and the intricate, lived experiences of neurodivergent individuals. Through an exhaustive exploration, the study advocates for a profound reassessment of legal, societal, and technological paradigms. Such a reevaluation aims to foster a more inclusive and compassionate conceptualization of accessibility, one that transcends mere design considerations to engage with the vast array of human experiences and needs.

1. Invisible Disabilities

The scholarship on disabilities and their legal protection has largely focused on physical disability. For instance, episodic disabilities denote lifelong health conditions that exert a considerable influence on the capability of an individual to engage in employment and various other social facets. In a Canadian study, McKee et al. (2006) characterizes episodic disability as «a serious mental or physical condition characterized by fluctuating periods and degrees of wellness and impairment. These periods are often unpredictable in severity, duration and potential for resolution» (p. 35). Further elucidating the nature of episodic disability, Boyce asserts, «an episodic disability can be permanent or temporary,

life-threatening or chronic, progressive or stable. What makes disability 'episodic' is that it produces recurring, sometimes cyclical, usually unpredictable periods of good and poor health» (p. 45). Boyce contends that compared to those with different forms of disability, individuals with episodic impairments encounter a unique disadvantage due to the longstanding inadequacy in the conceptualization, articulation, and address of this specific impairment within the frameworks of disability policies and programs (p. 34). Organizations focusing on episodic disability serve individuals living with an array of conditions, including but not limited to arthritis, specific types of cancer, Crohn's disease, diabetes, hepatitis C, HIV/AIDS, mental illness, mood disorders, and multiple sclerosis.

Alternatively, the delineation between visible disability and invisible disability hinges on the observability of the impairment. While a person with a visible disability exhibits an impairment that is readily perceptible to others, invisible disabilities remain concealed, lacking physical characteristics or behaviors that render them apparent. Since these impairments remain relatively hidden, they do not automatically transmit information about the individual to others, nor do they delineate a situation or mold initial anticipations during social encounters. The health condition or impairment does not conspicuously alter the appearance or demeanor of an individual, leading to a situation where the disability remains undetected and unrevealed in social interactions. Implicit in this understanding is the notion that there may be a concomitant absence of discriminatory or stereotypical reactions towards the individual (Prince, 2017).

Invisible disability, however, is not classified as a definitive clinical category or a separate social identity. Rather, some scholars propose a conceptualization that places visible and invisible disabilities on a continuum of conditions and particular contexts. Mollow (2010) accentuates «the impossibility of any absolute binary between 'visible' and 'invisible' disabilities» (p. 502), highlighting the complexity inherent in this dichotomy. A condition that might be concealed from a casual observer in a social context may become discernible to healthcare professionals through diagnostic evaluations. Mollow enumerates conditions such as "mental illnesses; some cognitive disabilities; and physical conditions such as chronic fatigue syndrome, repetitive strain injury, Environmental illness, and fibromyalgia, which don't produce objectively observable bodily changes" as constituting invisible disabilities (p. 502). In addition, certain gendered dimensions exist in relation to the perceptibility or concealment of impairments. For instance, Krogh and Johnson (2006) posit that women with disabilities are more susceptible to experiencing non-visible impairments, such as chronic illness and fatigue, compared to their male counterparts. This multifaceted understanding of invisible disabilities underscores the nuanced nature of how impairments manifest and are perceived across different contexts and demographics.

Specific to the study at hand, autism spectrum condition (ASC) (previously autism spectrum disorder (ASD) covers a range of invisible disabilities, including ADHD, dyslexia, dysgraphia and dyscalculia (Hodges et al., 2020). The stigma of a diagnosis has been pointed to as another reason an employee does not disclose in fear of further alienation

(Hurley-Hanson et al., 2020). Moreover, the symptomatic experiences that workers within the ASC may encounter is a multifaceted and complex matter, which requires attention to various cognitive and speech-related facets. In the realm of cognitive disabilities, a significant percentage of individuals experience restricted comprehension. Limitations in comprehension may manifest in an inability to grapple with intricate concepts, metaphors, or abstract language; or in difficulties understanding certain idiomatic expressions or slang (Smith & White, 2020). Paradoxically, some individuals may display extraordinary abilities in specific cognitive domains, such as numerical memory, even while struggling with more fundamental areas like social skills or emotional perception (McCauley et al., 2020). The dichotomy between these high and low cognitive functions highlights the heterogeneity and complexity of cognitive disabilities within the context of ASC.

Furthermore, the phenomenon of low tolerance for cognitive overload constitutes a critical aspect of cognitive disabilities. Individuals who are prone to cognitive overload may react with frustration or distress to multifaceted situations or an environment replete with simultaneous stimuli (Higgins et al., 2021). The need for simplicity and straightforwardness in their surroundings is paramount; an overabundance of choices or complexity can result in a paralyzing inability to act or a protracted emotional disturbance (Hutson & Hutson, 2023). Turning to the domain of speech disabilities, a wide array of conditions presents additional challenges. Stuttering, characterized by involuntarily repeated, prolonged, or blocked speech sounds, affects the fluency of speech (Kharismadewi et al., 2023). Similarly, “cluttering,” sometimes classified as a language disability, disrupts fluency through rapid, rhythmically inconsistent, and syntactically disorganized speech (Maruthy & Kelkar, 2023). Both Apraxia, a motor speech disability marked by difficulty in forming speech sounds, and Dysarthria, resulting from brain damage and leading to slurred or slow speech, further illustrate the multifaceted nature of speech disabilities within the ASC spectrum (Shriberg et al., 2019).

Articulation disorders, phonemic disorders, and non-vocal challenges constitute additional layers of complexity. Articulation disorders pertain to the physical production of speech sounds, resulting in omissions, additions, substitutions, or distortions (Griffen et al., 2022). Phonemic disorders, on the other hand, revolve around difficulties in distinguishing speech sounds, affecting word meaning and communication. Non-vocal disabilities, characterized by an utter inability to produce speech, emphasize the breadth and depth of invisible disabilities that may be encountered by ASC workers (van Rensburg et al., 2020).

Collectively, these observations underscore the intricate and diverse nature of invisible disabilities, both cognitive and speech-related, within the ASC context. The acknowledgment and understanding of these challenges necessitate a nuanced approach to supporting individuals in both personal and professional environments, emphasizing empathy, accommodation, and recognition of the inherent humanity of these so-called «special» needs.

2. Legal Protection

The Americans with Disabilities Act (ADA) has demonstrated efficacy in the establishment of building standards that furnish accessible spaces for individuals with physical impairments (Morgan, 2021). However, these guidelines have neglected the unique needs of those with mental, emotional, and developmental disabilities, including autism spectrum condition (ASC). Legal protections for individuals with disabilities constitute a complex landscape, marked by an interplay between civil rights, procurement regulations, industry-specific laws, and various tiers of governmental legislation, both domestic and international. These protections aim to ensure accessibility, equality, and non-discrimination across various facets of life, but often overlook the population under review here (Hawkins, 2023).

Civil rights laws serve as the foundation for legal protections, emphasizing the equal rights of persons with disabilities. These laws commonly prohibit discrimination in diverse contexts such as employment, accessibility to buildings, government services, and public accommodations, including eateries, retail, and entertainment venues. Notably, the ADA exemplifies a civil rights law that seeks to eradicate discrimination against individuals with disabilities, providing technical standards in some instances, while omitting them in others (Murphy, 2020).

Procurement laws represent another essential category, focusing on accessibility considerations in the acquisition of products or the contracting of services. Under such statutes, accessibility standards must be met, particularly by government entities. For example, Section 508 of the Rehabilitation Act in the United States and EN 301 549 in the European Union mandate that only products meeting accessibility criteria be considered for purchase. These laws significantly influence both governmental and private business purchasing decisions (Bosio et al., 2022).

Industry-specific laws introduce another layer of complexity, tailored to particular sectors deemed vital to accessibility. In the United States, the 21st Century Communications and Video Accessibility Act (CVAA) governs telecommunications, while the Air Carrier Access Act (ACAA) regulates airplane travel (Burks, 2013). These laws underscore the recognition that different industries may necessitate distinct and carefully crafted legal measures to ensure accessibility.

At the nexus of federal, state, and international laws, a comprehensive framework emerges to require accessibility for websites and Information Communications Technology (ICT) (Nath & Liu, 2017). The ADA mandates accessibility for various digital platforms and customer services, including sales, entertainment, and education. The CVAA expands upon this by encompassing communications products, services, and devices (Brooks, 2017). U.S. Section 508 of the Federal Rehabilitation Act, along with related state laws, mandates the procurement of the most accessible technology within the public sector (Olalere & Lazar, 2011). Specific state laws, such as Disabled Persons Act and Unruh Act of California, further enhance this landscape, complemented by international ADA-like

laws in countries like Korea, Canada, the U.K., and Australia (Schoen, 2022). The European Accessibility Act, presently in drafting stages, promises to have broad implications on products, services, and devices across the European Union.

Additionally, an important distinction should be made between the ADA and Section 508 of the Rehabilitation Act stand out as significant, yet distinctly different legislative instruments. An examination of both will shed light on their unique characteristics and contributions to the broader landscape of disability rights (Taylor & Bicak, 2021). The ADA represents a comprehensive civil rights law aimed at eliminating discrimination against individuals with disabilities across various spheres of public life in the United States (Schall, 1998). This act is subdivided into five major titles, each addressing specific domains:

Title I – Employment. This section emphasizes the prohibition of discrimination in all aspects related to employment, including hiring, firing, advancement, compensation, and training.

Title II – Public Services, State, and Local Government. This title focuses on non-discrimination in all programs, services, and activities offered by public entities.

Title III – Public Accommodations and Services Operated by Private Entities. This encompasses private places of public accommodation, including a wide array of establishments such as hotels, restaurants, and movie theaters.

Title IV – Telecommunications. This section mandates the provision of services facilitating communication over the telephone for people with hearing and speech disabilities and includes regulations on closed captioning.

Title V – Miscellaneous Provisions. This title captures various miscellaneous aspects related to the ADA, including its relationship with other laws, state immunity, and provisions on illegal drug use and attorney's fees.

Contrastingly, Section 508 of the Rehabilitation Act is a specific federal law mandating accessibility in electronic and information technology (EIT) employed by the federal government. This encompasses websites, software, hardware, electronic documents, and more (Jaeger, 2008). Its relevance to web accessibility was enhanced in January 2017 when the Web Content Accessibility Guidelines (WCAG) level A and AA were incorporated, replacing a modified subset of WCAG 1.0 (Caldwell et al., 2008). European legislation such as EN 301 549 shares similarities with Section 508, focusing on accessibility requirements for public procurement of Information and Communication Technology (ICT) products and services (Kous et al., 2021).

The critical differences between the ADA and Section 508 of the Rehabilitation Act can be clearly articulated by examining four key dimensions. In terms of technology, the ADA does not extensively address modern digital technology, whereas Section 508 has specific provisions relating to accessibility within this domain. The scope of the ADA is considerably broader, encompassing all areas of public life; in contrast, Section 508's focus is more

confined, targeting federal electronic and information technology exclusively. With regard to applicability, the ADA's reach extends to a wider range of entities, such as employers, governments, and businesses open to the public, while Section 508's applicability is primarily centered on federal agencies and those entities receiving federal funding or contracts. Finally, the enforcement mechanisms for these two laws are markedly different: under the ADA, any individual who believes they have faced discrimination can file a complaint, while under Section 508, grievances must be lodged with the particular federal department or agency responsible for the non-compliant electronic technology or information.

The comparison of the two acts highlights the complex legal landscape that individuals with ASC must navigate in the workplace. The critical distinctions between these two laws manifest in four key dimensions, each bearing significant implications for workers with autism and their protective rights. In the realm of technology, the lack of comprehensive provisions in the ADA for modern digital technology creates a potential void in the protection and support for individuals with ASC, who may require specific technological accommodations. Alternatively, the provisions of Section 508 targeting accessibility within the digital domain may, in some contexts, address these needs; however, its focus is confined exclusively to federal electronic and information technology, limiting its impact.

With regard to scope, the broader encompassment of all public life with the ADA might theoretically offer more substantial protection for workers with ASC. Conversely, the more narrow concentration of Section 508 potentially leaves gaps in addressing the unique needs of these individuals outside federal agencies. In terms of applicability, the former's wide reach, extending to employers, governments, and public businesses, seems to promise a more comprehensive coverage for workers with ASC. Yet, the latter's focus on federal agencies and those with federal funding or contracts may exclude significant sectors of employment from its purview, further marginalizing individuals with ASC within the workplace.

Finally, the distinct enforcement mechanisms between the two laws present additional challenges. The allowance for individual complaints with ADA regarding discrimination offers a direct avenue for redress. In contrast, Section 508's more convoluted grievance process, requiring complaints to be lodged with specific federal departments or agencies, may create barriers to justice for individuals with ASC who encounter non-compliance in the realm of electronic technology or information. Collectively, these dimensions paint a complex and often incongruent picture of the legal rights and protections afforded to workers with autism. The interplay and disparities between the ADA and Section 508 reveal an urgent need for a cohesive and nuanced approach that fully acknowledges and addresses the specific and multifaceted needs of individuals with ASC in the workplace. Such an approach requires a comprehensive reevaluation of existing legal frameworks, coupled with a robust commitment to fostering an inclusive and empathetic workplace culture that transcends mere legal compliance.

3. Support in Action

Other research has related the inadequacies of accommodations for the population under discussion post-pandemic. Capuano (2022), for instance, looked at the profound transformations in work patterns instigated by the COVID-19 pandemic and the concomitant challenges this presents to lawmakers and policymakers in Australia. The research and data examined in the article project a trend towards predominantly hybrid and shared workplaces in the post-pandemic era. A critical argument advanced in the article is that this paradigm shift in workplace design harbors specific risks of inequality and indirect discrimination based on invisible disability. Such a mode of working has been identified as inherently disadvantageous to employees with invisible disabilities, leading to new strata of workplace inequality. The analysis of Australian labor law and anti-discrimination law reveals that current legal structures are inadequately prepared to tackle these emerging inequalities. Thus, the existing law falls short in addressing the challenges faced by employees with invisible disabilities in the contemporary and post-pandemic workplace landscape. Furthermore, when employees with invisible disabilities attempt to establish adverse action under the Fair Work (FW) Act or indirect discrimination under existing legislation, their claims are often unjustly defeated. This is attributed not to the lack of merit in the claims but to deficiencies within the legal system itself. Proposals for reforming the FW Act and various state and territory anti-discrimination statutes are advocated, aiming to afford claimants with invisible disabilities equal coverage to those with visible disabilities (Farbenblum & Berg, 2017).

Along the same lines, and in light of the growing prevalence of autism diagnoses, there emerges an imperative for designers and architects to broaden their planning horizons to incorporate more universally applicable solutions. As such, Clouse et al. (2020) presented methodologies for designing beyond the ADA framework to cater to the needs of individuals with ASC. To achieve such a design, those in the architectural and design professions must recognize and address sensory challenges that could impede the ability of those with the condition to attain a regulatory state, thereby facilitating their effective interaction with neurotypical peers. Additionally, design considerations extend to teachers, therapists, and parents of children with autism to foster more successful interactions. An environment that overstimulates a child with ASD may impede the efforts of parents, caregivers, or therapists in realizing their respective goals.

One potential solution Mostafa advanced are seven design criteria, encapsulated in the acronym ASPECTSS, which stands for Acoustics, Spatial sequencing, Escape spaces, Compartmentalization, Transition spaces, Sensory zoning, and Safety (Mostafa, 2014). These criteria, specifically tailored for individuals with ASD, form the foundational principles for the established guidelines. As designers and architects, there resides an ethical obligation to fabricate inclusive environments. To this end, the authors spotlighted a vocational center, juxtaposing one plan that conforms to ADA guidelines with another that embodies supplementary environmental features catering to the needs of people with ASD. These design criteria, derived from a synthesis of evidence-based solutions procured

through a comprehensive literature review and personal interviews, underscore the sentiment that a sensitive approach to the needs of individuals with autism not only provides targeted solutions but enhances the built environment for all. It is a profound testament to the potential for design to transcend mere compliance and aspire to inclusivity and empathy.

Laws pertaining to disability accommodations, notably within the workplace, have historically been rooted in architectural or physical design considerations (Hawkins, 2023; Murphy, 2020). This perspective has shaped the legislation, informing guidelines and requirements primarily focused on rendering physical spaces accessible. From ramps and elevators to accessible restrooms, these tangible provisions have become emblematic of disability accommodations. However, this traditional approach overlooks a pivotal aspect of contemporary work-life: the digital domain.

4. Recommendations

In the modern workplace, a significant portion of daily interaction and job-related tasks have transitioned to digital platforms (Baptista et al., 2020). Activities such as typing on a keyboard, reading from a screen, or engaging in virtual meetings constitute an integral part of the work experience. Consequently, the accessibility landscape has fundamentally evolved, necessitating a reevaluation of existing legal frameworks. Thus, the present emphasis on architectural accommodations fails to capture the complexity of the digital environment, wherein accessibility may pertain to factors such as screen readability, keyboard functionality, or the cognitive demands imposed by user interfaces. For individuals with various disabilities, including neurodivergent conditions, these digital interactions may present barriers as significant as physical obstacles. Yet, prevailing legislation tends to lag in acknowledging and addressing these digital accessibility considerations (Inal et al., 2020).

The disconnect between traditional legal perspectives on disability accommodations and the emergent needs of the digital workplace illuminates a profound gap in the accessibility discourse. While architectural considerations undoubtedly remain essential, they no longer suffice as the exclusive focus of disability accommodations. The transition to a digitally-driven work environment calls for a comprehensive understanding of accessibility that extends beyond physical design to encompass the multifaceted nuances of digital inclusivity (de Melo et al., 2022). Such an understanding demands a proactive and informed approach to legislation, one that recognizes and responds to the dynamic nature of contemporary work practices and the diverse spectrum of human abilities and needs. The realization sets the stage for the exploration of recommendations that seek to bridge this gap, fostering a more inclusive and responsive legal, societal, and technological landscape.

Previous studies have outlined strategies to promote neuroinclusivity in the workplace. The accommodation of neurodivergent workers in contemporary work environments necessitates a significant shift from conventional practices. Recommendations for this transformation pivot around the principle of individualized, person-centered communication. Emphasizing explicit, well-defined guidelines, managers and colleagues are encouraged

to provide step-by-step instructions that minimize ambiguity and enhance comprehension. Sensitivity to work and communication preferences, such as offering clear timelines for projects and giving advance notice of meetings, fosters a supportive and predictable environment. Literal and direct instructions, devoid of abstract or ambiguous language, further contribute to clarity. Visual aids to reinforce key points and pre-meeting agendas align with diverse cognitive processing needs. Furthermore, recognizing the unique social interaction dynamics of neurodivergent individuals, recommendations include curtailing small talk, offering conversational exits, and considering the optional nature of camera usage in video conferences. Collectively, these recommendations coalesce into a comprehensive framework that acknowledges the distinctive needs and preferences of neurodivergent workers. This approach not only facilitates effective communication and collaboration but also reflects a profound respect for neurodiversity, enabling workplaces to transcend conventional norms and create a more inclusive, empathetic, and productive environment (Hutson & Hutson, 2023).

While previous recommendations focus on environmental considerations, digital accessibility accommodations should now be the primary focus given the nature of work in the Digital Age. At the same time, the multifaceted approach required to establish digital inclusivity needs to focus on five distinct thematic areas- perceivability, operability, understandability, robustness and specific technical measures- each of which plays a pivotal role in accommodating neurodivergent individuals within digital environments.

Perceivability within the context of digital design for neurodivergent individuals represents a multifaceted endeavor. The ultimate goal of enhancing perceivability is to make digital content accessible in various forms that cater to diverse perceptual needs. Providing text alternatives for non-text content exemplifies one avenue towards achieving perceivability. For example, including transcripts for video content allows those with auditory impairments to access the information, and providing alt text descriptions for images ensures that visually impaired users can comprehend visual content through screen readers (Kous et al., 2020). These text alternatives may further be converted into braille, speech, or large print, enhancing accessibility across various mediums.

Similarly, time-based media such as videos and animations must be complemented with alternatives like captions or sign language interpretation. A clear example can be seen in educational platforms that offer subtitled lectures, enabling both hearing-impaired individuals and non-native speakers to follow the content more effectively. Also, the arrangement of content on a webpage is essential in maintaining the integrity and structure of the information when presented in different formats (Duarte & Fonseca, 2019). For instance, utilizing flexible grid layouts ensures that content remains coherent when resized or rearranged for mobile viewing. This flexibility caters to users who may require larger text sizes or specific color contrasts, without compromising the overall structural integrity of the content (Lister et al., 2020).

Another pivotal aspect of perceivability lies in distinguishing between the background and foreground to enhance both visibility and auditory comprehension. An illustrative example can be found in websites that offer a 'dark mode,' catering to users who find bright backgrounds visually straining (Willmore & King, 2023). Additionally, ensuring clear

and distinct audio channels in multimedia content aids individuals who might struggle with auditory processing, allowing them to differentiate between multiple sound sources easily. Perceivability also entails multisensory engagement. For instance, incorporating tactile feedback in touchscreen interfaces can provide valuable cues to individuals with visual impairments. Haptic technology, which simulates touch sensations, represents an innovative avenue that broadens accessibility by engaging multiple senses (Michelsanti et al., 2021).

Operability within the context of digital design signifies the capacity to engage with and navigate digital content effectively. This concept encompasses various components, and it is paramount for ensuring an inclusive experience for neurodivergent individuals and other disabilities. A primary consideration within operability is the accessibility of all functionalities through diverse inputs, not confined solely to a keyboard. This includes alternative input methods such as voice commands, touch gestures, or eye-tracking technologies (Lowndes & Connelly, 2023). For example, voice recognition software like Dragon NaturallySpeaking provides individuals with mobility impairments the ability to navigate and control applications through voice commands (Vickers et al., 2022). Meanwhile, adaptive technologies like eye-tracking allow users with limited motor control to interact with digital content through eye movements.

Providing users with enough time to consume and interact with content is essential. Consider a banking website that utilizes timed sessions for security purposes; implementing features that allow users to request additional time ensures that those who may require longer to read or navigate are not prematurely logged out. Furthermore, adjustable playback speed in video content is a valuable feature, enabling users to consume media at a pace suited to their comprehension and comfort (Seo et al., 2021). At the same time, effective navigation is a cornerstone of operability. Incorporation of features such as breadcrumb trails, clear headings, consistent navigation menus, and descriptive link texts fosters an intuitive user experience. For instance, websites that provide 'skip to content' links enable screen reader users to bypass repetitive navigation links, facilitating quicker access to the main content (Pham et al., 2023).

Careful attention must be paid to the design elements that might cause seizures. The incident involving a Pokémon episode causing seizures in 685 children, as highlighted in the Seizure Prevention Guidelines (1997), serves as a poignant reminder of the potential risks associated with rapid flashing visuals or specific color patterns. Modern web design guidelines often stress adherence to safe color contrasts and limiting the frequency of flashing elements to avoid such health risks. Therefore, responsiveness to individual user preferences further illustrates the depth of consideration required for operability (Ferlazzo et al., 2021). Features like customizable font sizes, color schemes, or layout options empower users to tailor the interface to their specific needs. For example, platforms like BBC's My Web, My Way[1] allow users to set their preferences for text size, color, and other display options, enhancing readability and comfort. In all, operability

[1] https://goo.su/ynhV7

within digital design transcends mere functionality; it embodies a user-centric approach that acknowledges and accommodates the diverse needs and preferences of all users (Proença et al., 2021).

Understandability, in the context of digital design, denotes the ease with which users can interpret, comprehend, and engage with the content. For individuals with cognitive disabilities, including those with ASC, factors affecting understandability can profoundly impact their experience and ability to navigate digital environments. The following delineates various aspects of understandability, providing examples to illuminate their significance (Zubala et al., 2021). For instance, ensuring that the text is easily readable is foundational to understandability. Factors such as font size, typeface, line length, and color contrast play crucial roles in readability. For example, websites employing dyslexia-friendly fonts and sufficient spacing between lines cater to the unique reading needs of individuals with dyslexia. Furthermore, adherence to WCAG (Web Content Accessibility Guidelines) contrast ratios, as tested by tools like accessiBe, can make the difference between text being legible or indecipherable for users with visual impairments (Panda & Chakravarty, 2020).

Employing semantic headings and maintaining a logical structure contribute to the ease of navigation and comprehension. Properly nested headings (e.g., H1 followed by H2, H3) not only create a visual hierarchy for sighted users but also allow screen readers to interpret the content's structure, facilitating navigation for visually impaired users. Additionally, clear section divisions and a consistent layout enable users to predict where information is likely to be found, reducing cognitive load (Fayyaz & Khusro, 2023). Along the same lines, Accessible Rich Internet Applications (ARIA) landmarks provide critical support for assistive technologies, defining distinct regions of web content such as banners, main content, navigation, and search. For example, by marking the main content area with the ARIA role=»main», screen reader users can directly navigate to that section, bypassing repetitive navigation links. This targeted navigation enhances efficiency and comprehension for users relying on assistive technology (Blanco et al., 2022).

Providing clear guidance to prevent errors and aiding users in correcting mistakes enhances understandability. For instance, an e-commerce site might employ real-time validation on forms, highlighting incorrect fields and providing specific error messages like «Invalid email format.» Such immediate feedback supports users in understanding and rectifying errors without confusion or frustration. Ensuring that web pages operate in a predictable manner minimizes confusion and cognitive overload. This can include consistent navigation menus across different sections of a site, predictable responses to user actions (such as clicking a button), and clear warnings for significant changes, like opening a new window or tab. Automated tools such as Keros facilitate adherence to understandability principles through features like color contrast analysis, ensuring

that designers adhere to best practices and standards without requiring specialized knowledge in accessibility (Teh & Ramli, 2023). Thus, understandability as a dimension of digital design involves an intricate balance of visual aesthetics, content structure, user guidance, and technological support. By employing practices such as semantic headings, ARIA landmarks, and automated testing, designers and developers can create digital environments that are not merely accessible but comprehensible and engaging for all users, including those with cognitive disabilities (Blanco et al., 2022).

Robustness in digital design refers to the resilience and adaptability of a system in providing a consistent user experience across various platforms and technologies, including assistive tools. This attribute extends beyond mere functional operability to encompass a nuanced integration of visual aesthetics and functional accessibility. Here, an exploration of key elements that contribute to robust design is presented, complete with examples to elucidate the practical implementation of these principles. In designing for robustness, accommodations must be made for individuals who may rely on one-handed keyboard navigation. This can include those with temporary conditions such as a broken arm or more permanent disabilities affecting hand usage. Websites and applications that support key commands, shortcuts, and tab navigation enhance the user experience for this demographic. For instance, the application of 'Sticky Keys' in operating systems allows sequential rather than simultaneous key presses, facilitating one-handed operation. The application of this accessibility feature in computing environments has garnered significant attention due to its potential to enhance the user experience for individuals with physical disabilities or motor impairments (Thompson & Copeland, 2020).

The provision of alt text for images ensures that content remains accessible to users who rely on screen readers or have images turned off, as in some low-bandwidth environments. Descriptive alt text, such as «A group of employees collaborating around a conference table,» provides context and information, maintaining content richness and meaning. This approach aligns with the principle of robustness, ensuring that visual content remains perceivable across diverse user experiences. Likewise, incorporating invisible labels for form elements enhances accessibility without disrupting visual design. These labels are hidden visually but accessible to screen readers, enabling users with visual impairments to understand and interact with forms. An example would be a login form where the fields «Username» and «Password» are visually hidden but still narrated by assistive technologies (Gleason et al., 2020).

Tables can present complex data in an easily digestible format, but without careful design, they can become a barrier for users with disabilities. Utilizing appropriate table headers and ensuring proper row and column associations make the information accessible to screen readers. Tools such as the 'scope' attribute within HTML define relationships between headers and cells, making the information comprehensible for users relying on assistive technologies. Robust design entails not only compliance with current

technologies but also consideration of future advancements. Utilizing standard coding practices, avoiding deprecated elements, and testing across various browsers and devices ensure that content remains accessible and consistent over time. Moreover, compliance with evolving standards like WCAG ensures alignment with best practices in accessibility (Zhang & Balog, 2020).

Robustness transcends technical specifications to become a collaboration between aesthetics and functionality. The seamless integration of visual design with user-centered considerations reflects a holistic approach to accessibility that accommodates various inputs, user preferences, and technological environments. By implementing strategies such as one-handed keyboard accessibility, alt text, invisible labels, and standards-compliant coding practices, designers and developers can create resilient and adaptable digital experiences. Such robust design not only ensures legal compliance but also aligns with ethical considerations, emphasizing the dignity and diversity of all users.

Specific Technical Measures, as the final thematic area in enhancing digital inclusivity, encompass a variety of specialized techniques that serve to augment accessibility. This domain represents a synthesis of components that require careful attention to detail. In the realm of accessibility, comprehensive solutions must be tailored to meet individual needs. Here, an exploration of specific technical measures, including examples, helps to delineate this complex domain. To begin with, the Accessible Rich Internet Applications (ARIA) suite provides a way to make web content more accessible to people with disabilities. ARIA's role, state, and property attributes can be added to HTML, thereby enhancing the accessibility of JavaScript widgets like sliders, menus, and dialog boxes (Chiou et al., 2021). For instance, by integrating ARIA roles such as «slider» or «button,» developers can ensure that assistive technologies like screen readers interpret these widgets correctly.

Other accessible considerations include adequate color contrast between text and background is critical for individuals with visual impairments, including color blindness. Tools such as the WebAIM color contrast checker can assess and ensure appropriate contrast ratios, in line with WCAG guidelines. For example, ensuring that text color has a 4.5:1 contrast ratio against its background can make reading more comfortable for users with low vision (Frey & Mancilla, 2023). A similar consideration should be made on social media platforms have become integral to modern communication, and accessibility within these platforms is vital. Strategies such as providing image descriptions on Twitter[2] or using camel case in hashtags (e.g., #DigitalAccessibility) enhance readability for screen readers (Kausar et al., 2021). These practices enable users with visual or cognitive disabilities to engage fully with social media content.

[2] A social network blocked in the territory of the Russian Federation for disseminating illegal information.

This approach involves enhancing the HTML syntax with WAI-ARIA attributes to provide additional accessibility information. Utilizing roles, states, and properties that define accessible relationships between elements ensures compatibility with assistive technologies. The realm of specific technical measures in digital accessibility requires a nuanced understanding and careful execution of various strategies (Table 1). From ARIA integration to social media accessibility, each component plays a vital role in crafting an inclusive digital experience (Žuličeк et al., 2021). By adopting these practices, developers and designers can construct web content that is not only compliant with legal standards but also responsive to the multifaceted needs of all users.

Table 1. Factors for Enhancing Digital Accessibility for Neurodivergent Individuals

Factor	Associated Recommendations for Digital Accessibility
Perceivability	– Provide text alternatives for non-text content (e.g., braille, speech). – Offer alternatives for time-based media. – Arrange content to allow different presentations without loss of information. – Enhance background and foreground separation for visibility and auditory comprehension
Operability	– Ensure all functionalities are accessible via various inputs (keyboard, touch, voice, etc.). – Provide users ample time to consume content. – Prevent design elements that may cause seizures. – Facilitate navigation and content finding
Understandability	– Ensure text readability and web page predictability. – Employ semantic headings and utilize ARIA landmarks. – Use tools like Keros for color contrast analysis
Robustness	– Facilitate interaction through strategies like one-handed keyboard accessibility. – Use alt text for images and invisible labels for form elements. – Ensure compatibility with current and future user agents, including assistive technologies. – Use appropriate table headers and other design elements without altering visual design
Specific Technical Measures	– Integrate ARIA for JavaScript widgets. – Ensure color contrast consideration, e.g., with WebAIM Color Contrast Checker. – Enhance social media accessibility, including image descriptions and camel case in hashtags. – Provide links to skip navigation. – Consider cognitive disabilities in design. – Integrate WAI-ARIA into HTML syntax for compatibility with assistive technologies

In the effort to create an inclusive and accessible digital environment for neurodivergent individuals, an extensive consideration of the five salient factors – perceivability, operability, understandability, robustness, and specific technical measures – offers a structured approach to addressing diverse needs. The recommendations delineated within this discourse illuminate the myriad dimensions that must be addressed to ensure

the comprehensive inclusion of all users, regardless of their neurodivergent status. Embracing such a multifaceted approach resonates with the broader commitment to fostering inclusivity and equality in the virtual world. The confluence of visual aesthetics, functional accessibility, and meticulous attention to detail encapsulates a universally designed user experience that transcends mere compliance with existing standards. The pursuit of these principles, illuminated through specific examples and expert insights, establishes a foundation for designers, developers, and policymakers to create a future where the digital realm is an extension of societal values of inclusivity and empathy. The future of digital design lies in recognizing and embracing the inherent diversity of human experience, and the articulated recommendations offer a blueprint for such an enlightened path.

Conclusion

The analysis herein turns attention toward the significant concern of invisible disabilities in the workplace and the implications surrounding Autism Spectrum Condition (ASC). In doing so, the discourse emphasizes a critical examination of the current limitations of the Americans with Disabilities Act (ADA) and contemplates the recommendations as detailed in a specified article. This intricate synthesis culminates in an articulation of the next steps for research, thus fortifying the understanding of this multifaceted subject matter.

Invisible disabilities in the workplace represent a complex challenge that often goes unrecognized. These disabilities, which include conditions such as ASC, are not readily apparent but can significantly impact the ability of an individual to function in a traditional workplace environment. The ramifications of this issue extend to the broader theme of inclusivity, as it poses the question of how workplaces can foster an environment where all employees, regardless of any invisible disabilities, can thrive. Concerning the ASC, and neurodivergence in particular, the nuances become more complex, particularly considering the broad range of manifestations and how they might interact with the workplace environment. There is a necessity to appreciate the unique strengths and challenges of individuals with ASC and to create supportive structures tailored to these unique characteristics. This necessitates an acknowledgment that the workplace must extend beyond mere accommodation and work towards a more inclusive and embracing environment.

However, the limitations of the existing ADA legislation become evident within this context. The ADA, although pioneering in its vision, has been found to be insufficient in addressing the specific needs of those with invisible disabilities, including ASC. The focus of the act on physical accessibility sometimes overshadows the nuanced requirements of those with cognitive or developmental disabilities, leading to gaps in accommodation and support. The recommendations outlined in the article under consideration serve to address some of these gaps. These suggestions emphasize a reevaluation of the existing legal framework, a call for more extensive collaboration between employers and disability advocates, and the importance of creating supportive

community networks. However, these recommendations are not without challenges, and implementing them requires a careful and thoughtful approach that considers the complex interplay of individual needs, organizational culture, and legal requirements.

The way forward, therefore, must entail a multifaceted research agenda that aligns with the aforementioned challenges and recommendations. Future research should delve into an empirical examination of workplace practices in accommodating invisible disabilities, including ASC. There is also an immediate need for legal scholarship that critically evaluates the effectiveness of ADA in the context of invisible disabilities and recommends possible amendments or supplements. Additionally, an interdisciplinary approach, engaging with fields such as psychology, sociology, organizational behavior, and law, will be instrumental in creating a more nuanced understanding. Furthermore, collaboration with organizations, disability advocates, and individuals with disabilities will provide a more authentic and grounded perspective.

References

Baptista, J., Stein, M. K., Klein, S., Watson-Manheim, M. B., & Lee, J. (2020). Digital Work and Organisational Transformation: Emergent Digital/Human Work Configurations in Modern Organisations. *The Journal of Strategic Information Systems*, *29*(2), 101618. https://doi.org/10.1016/j.jsis.2020.101618

Blanco, M., Zong, J., & Satyanarayan, A. (2022). *Olli: An Extensible Visualization Library for Screen Reader Accessibility*. https://vis.mit.edu/pubs/olli.pdf

Bosio, E., Djankov, S., Glaeser, E., & Shleifer, A. (2022). Public Procurement in Law and Practice. *American Economic Review*, *112*(4), 1091–1117. https://doi.org/10.1257/aer.20200738

Brooks, A. (2017). Accessibility: Definition, Labeling, and CVAA Impact. *Recent Advances in Technologies for Inclusive Well-Being: From Worn to Off-body Sensing, Virtual Worlds, and Games for Serious Applications*, 283–383. https://doi.org/10.1007/978-3-319-49879-9_14

Burks, C. L. (2013). Improving Access to Commercial Websites Under the Americans with Disabilities Act and the Twenty-First Century Communications and Video Accessibility Act. *Iowa Law Review, 99*(1), 363. https://clck.ru/36kuL4

Caldwell, B., Cooper, M., Reid, L. G., Vanderheiden, G., Chisholm, W., Slatin, J., & White, J. (2008). *Web Content Accessibility Guidelines (WCAG) 2.0. WWW Consortium (W3C)*, *290*, 1–34. https://clck.ru/36kuNe

Capuano, A. (2022). Post-Pandemic Workplace Design and the Plight of Employees with Invisible Disabilities: In Australian Labour Law and Anti-Discrimination Legislation Equipped to Address New and Emerging Workplace Inequalities?. *The University of New South Wales Law Journal*, *45*(2), 873–913. https://doi.org/10.53637/emwr6179

Chiou, P. T., Alotaibi, A. S., & Halfond, W. G. (2021, August). Detecting and Localizing Keyboard Accessibility Failures in Web Applications. In *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (pp. 855–867). https://doi.org/10.1145/3468264.3468581

Clouse, J. R., Wood-Nartker, J., & Rice, F. A. (2020). Designing Beyond the Americans with Disabilities Act (ADA): Creating an Autism-Friendly Vocational Center. *HERD: Health Environments Research & Design Journal*, *13*(3), 215–229. https://doi.org/10.1177/1937586719888502

de Melo, F. D. A. F., Soares, K. P., de Barros, E. M., dos Santos Cabral, E. L., da Costa Júnior, J. F., da Silva, A. A. R. S., & Burlamaqui, A. M. F. (2022). Inclusive Digital Technologies in the Classroom: A Case Study Focused on Students with Autism Spectrum Disorder (ASD) in the Final Years of Elementary School. *Research, Society and Development*, *11*(6), e10211628759-e10211628759. https://doi.org/10.33448/rsd-v11i6.28759

Duarte, C., & Fonseca, M. J. (2019). *Multimedia Accessibility. In Web Accessibility: A Foundation for Research* (pp. 461–475). Springer, London. https://doi.org/10.1007/978-1-4471-7440-0_25

Farbenblum, B., & Berg, L. (2017). Migrant Workers' Access to Remedy for Exploitation in Australia: The Role of the National Fair Work Ombudsman. *Australian Journal of Human Rights*, *23*(3), 310–331. https://doi.org/10.1080/1323238x.2017.1392478

Fayyaz, N., & Khusro, S. (2023). Enhancing Accessibility for the Blind and Visually Impaired: Presenting Semantic Information in PDF Tables. *Journal of King Saud University – Computer and Information Sciences*, 101617. https://doi.org/10.1016/j.jksuci.2023.101617

Ferlazzo, E., Sueri, C., Masnou, P., Aguglia, U., Mercuri, S., Caminiti, E., & Piccioli, M. (2021). Technical Issues for Video Game Developers and Architects to Prevent Photosensitivity. In *The Importance of Photosensitivity for Epilepsy* (pp. 407–412). Springer, Cham. https://doi.org/10.1007/978-3-319-05080-5_33

Frey, B. A., & Mancilla, R. (2023). Inclusive Online Learning: Digital Accessibility Practices. In *Diversity in Higher Education Remote Learning: A Practical Guide* (pp. 93–104). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-31214-4_8

Gleason, C., Pavel, A., McCamey, E., Low, C., Carrington, P., Kitani, K. M., & Bigham, J. P. (2020, April). Twitter A11y: A Browser Extension to Make Twitter Images Accessible. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–12). https://doi.org/10.1145/3313831.3376728

Griffen, B., Woods-Catterlin, L., Lorah, E. R., & Whitby, P. S. (2022). Teaching Communication to Individuals with Autism Spectrum Disorders. In *Autism Spectrum Disorders: Advancing Positive Practices in Education*. (5th Ed.). Routledge. https://doi.org/10.4324/9781003255147-9

Hawkins, D. S. (2023). Overlooked and Undercounted: Communication and Police Brutality Against People with Disabilities. In *The Palgrave Handbook of Disability and Communication* (pp. 385–399). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-14447-9_23

Higgins, J. M., Arnold, S. R., Weise, J., Pellicano, E., & Trollor, J. N. (2021). Defining Autistic Burnout Through Experts by Lived Experience: Grounded Delphi Method Investigating #AutisticBurnout. *Autism*, *25*(8), 2356–2369. https://doi.org/10.1177/13623613211019858

Hodges, H., Fealko, C., & Soares, N. (2020). Autism Spectrum Disorder: Definition, Epidemiology, Causes, and Clinical Evaluation. *Translational Pediatrics*, *9*(Suppl 1), S55. https://doi.org/10.21037/tp.2019.09.09

Hurley-Hanson, A. E., Giannantonio, C. M., Griffiths, A. J., Hurley-Hanson, A. E., Giannantonio, C. M., & Griffiths, A. J. (2020). The Stigma of Autism. *Autism in the Workplace: Creating Positive Employment and Career Outcomes for Generation A* (pp. 21–45). https://doi.org/10.1007/978-3-030-29049-8_2

Hutson, P., & Hutson, J. (2023). Neurodiversity and Inclusivity in the Workplace: Biopsychosocial Interventions for Promoting Competitive Advantage. *Journal of Organizational Psychology*, *23*(2), 1–16. https://doi.org/10.33423/jop.v23i2.6159

Inal, Y., Guribye, F., Rajanen, D., Rajanen, M., & Rost, M. (2020, October). Perspectives and practices of digital accessibility: A survey of user experience professionals in Nordic countries. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (pp. 1–11). https://doi.org/10.1145/3419249.3420119

Maruthy, S., & Kelkar, P. (Eds.). (2023). *Understanding and Managing Fluency Disorders: From Theory to Practice*. Routledge. https://doi.org/10.4324/9781003367673

Jaeger, P. T. (2008). User-Centered Policy Evaluations of Section 508 of the Rehabilitation Act: Evaluating E-Government Web Sites for Accessibility for Persons with Disabilities. *Journal of Disability Policy Studies*, *19*(1), 24–33. https://doi.org/10.1177/1044207308315274

Kausar, S., Tahir, B., & Mehmood, M. A. (2021, December). HashCat: A Novel Approach for the Topic Classification of Multilingual Twitter Trends. In *2021 International Conference on Frontiers of Information Technology (FIT)* (pp. 212–217). IEEE. https://doi.org/10.1109/fit53504.2021.00047

Kharismadewi, Y., Revita, I., & AS, R. M. (2023). A Praat-Based Stuttering Analysis of the Main Character in the King's Speech Movie: A Neuropsycholinguistic Study. *Journal of Applied Studies in Language*, *7*(1), 56–65. https://doi.org/10.31940/jasl.v7i1.56-65

Kous, K., Kuhar, S., Pavlinek, M., Heričko, M., & Pušnik, M. (2021). Web Accessibility Investigation of Slovenian Municipalities' Websites Before and After the Adoption of European Standard EN 301 549. *Universal Access in the Information Society*, *20*, 595–615. https://doi.org/10.1007/s10209-020-00732-9

Kous, K., Kuhar, S., Rajšp, A., & Šumak, B. (2020, September). Investigation of the Accessibility of Non-Text Content Published on Websites. In *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 1645–1650). IEEE. https://doi.org/10.23919/mipro48935.2020.9245288

Krogh, K., & Johnson, J. (2006). A Life without Living: Challenging Medical and Economic Reductionism in Home Support Policy for People with Disabilities. In *D. Pothier, & R. Devlin (Eds.), Critical disability theory: Essays in philosophy, politics, policy and law* (pp. 151–176). Vancouver: University of British Columbia Press. https://doi.org/10.59962/9780774851695-010

Lister, K., Coughlan, T., Iniesto, F., Freear, N., & Devine, P. (2020, April). Accessible Conversational User Interfaces: Considerations for Design. In *Proceedings of the 17th International Web for All Conference* (pp. 1–11). https://doi.org/10.1145/3371300.3383343

Lowndes, A. M., & Connelly, D. M. (2023). User Experiences of Older Adults Navigating an Online Database of Community-Based Physical Activity Programs. *Digital Health*, *9*. https://doi.org/10.1177/20552076231167004

Matthews, C. K., & Harrington, N. G. (2000). Invisible disabilities. In *D.O. Braithwaite, & T. L. Thompson (Eds.), Handbook of Communication and People with Disabilities: Research and Application* (pp. 405–421). New Jersey: Lawrence Erlbaum Associates, Inc.

McCauley, J. B., Pickles, A., Huerta, M., & Lord, C. (2020). Defining Positive Outcomes in More and Less Cognitively Able Autistic Adults. *Autism Research*, *13*(9), 1548–1560. https://doi.org/10.1002/aur.2359

McKee, E., Popiel, M., & Boyce, W. (2006). *Policies and Programs to Facilitate Labour Force Participation for People with Episodic Disabilities: Recommendations for a Canadian Context Based on an International Analysis*. Toronto: Canadian Working Group on HIV and Rehabilitation.

Michelsanti, D., Tan, Z. H., Zhang, S. X., Xu, Y., Yu, M., Yu, D., & Jensen, J. (2021). An Overview of Deep-Learning-Based Audio-Visual Speech Enhancement and Separation. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, *29*, 1368–1396. https://doi.org/10.1109/taslp.2021.3066303

Mollow, A. (2010). When Black Women Start Going on Prozac. In *L. J. Davis (Ed). The Disability Studies Reader* (3d Ed., pp. 486–506). New York: Routledge.

Morgan, J. N. (2021). Policing Under Disability Law. *Stanford Law Review*, *73*, 1401–1469.

Mostafa, M. (2014). Architecture for Autism: Autism ASPECTSS™ in School Design. *International Journal of Architectural Research: ArchNet-IJAR*, *8*(1), 143–158. https://doi.org/10.26687/archnet-ijar.v8i1.314

Murphy, K. L. (2020). Civil Rights Laws: Americans With Disabilities Act of 1990 and Section 504 of the Rehabilitation Act of 1973. *Journal of Physical Education, Recreation & Dance*, *92*(1), 57–59. https://doi.org/10.1080/07303084.2021.1844555

Nath, H. K., & Liu, L. (2017). Information and Communications Technology (ICT) and Services Trade. *Information Economics and Policy*, *41*, 81–87. https://doi.org/10.1016/j.infoecopol.2017.06.003

Neely, B. H., & Hunter, S. T. (2014). In a Discussion on Invisible Disabilities, Let Us Not Lose Sight of Employees on the Autism Spectrum. *Industrial and Organizational Psychology*, *7*(2), 274–277. https://doi.org/10.1111/iops.12148

Olalere, A., & Lazar, J. (2011). Accessibility of US Federal Government Home Pages: Section 508 Compliance and Site Accessibility Statements. *Government Information Quarterly*, *28*(3), 303–309. https://doi.org/10.1016/j.giq.2011.02.002

Panda, S., & Chakravarty, R. (2020). Evaluating the Web Accessibility of IIT Libraries: A Study of Web Content Accessibility Guidelines. *Performance Measurement and Metrics*, *21*(3), 121–145. https://doi.org/10.1108/pmm-02-2020-0011

Patton, E. (2022). To Disclose or Not Disclose a Workplace Disability to Coworkers: Attributions and Invisible Health Conditions in the Workplace. *Equality, Diversity and Inclusion: An International Journal*, *41*(8), 1154–1180. https://doi.org/10.1108/edi-09-2021-0228

Pham, M., Singh, K., & Jahnke, I. (2023). Socio-Technical-Pedagogical Usability of Online Courses for Older Adult Learners. *Interactive Learning Environments*, *31*(5), 2855–2871. https://doi.org/10.1080/10494820.2021.1912784

Prince, M. J. (2017). Persons with Invisible Disabilities and Workplace Accommodation: Findings from a Scoping Literature Review. *Journal of Vocational Rehabilitation*, *46*(1), 75–86. https://doi.org/10.3233/jvr-160844

Proença, M. D. Q., Motti, V. G., Rodrigues, K. R. D. H., & Neris, V. P. D. A. (2021). Coping with Diversity-A System for End-users to Customize Web User Interfaces. *Proceedings of the ACM on Human-Computer Interaction*, *5*(EICS), 1–27. https://doi.org/10.1145/3457151

Reeve, T., & Gottselig, S. (2011). *Investigating Workplace Accommodation for People with Invisible Disabilities, Research Report*. Vancouver: BC Coalition of People with Disabilities.

Schall, C. M. (1998). The Americans with Disabilities Act – are we keeping our promise? An analysis of the effect of the ADA on the employment of persons with disabilities. *Journal of Vocational Rehabilitation*, *10*(3), 191–203. https://doi.org/10.3233/jvr-1998-10303

Schoen, J. (2022). Patching Procedural Potholes in Supplemental Jurisdiction Claims Involving ADA & Unruh Act Litigation in California Federal Courts. *Loyola Law Review*, *55*(4), 1107–1132. https://clck.ru/36kuXG

Seo, K., Dodson, S., Harandi, N. M., Roberson, N., Fels, S., & Roll, I. (2021). Active Learning with Online Video: The Impact of Learning Context on Engagement. *Computers & Education*, *165*, 104132. https://doi.org/10.1016/j.compedu.2021.104132

Shriberg, L. D., Kwiatkowski, J., & Mabie, H. L. (2019). Estimates of the Prevalence of Motor Speech Disorders in Children with Idiopathic Speech Delay. *Clinical Linguistics & Phonetics*, *33*(8), 679–706. https://doi.org/10.1080/02699206.2019.1595731

Smith, I. C., & White, S. W. (2020). Socio-Emotional Determinants of Depressive Symptoms in Adolescents and Adults with Autism Spectrum Disorder: A Systematic Review. *Autism*, *24*(4), 995–1010. https://doi.org/10.1177/1362361320908101

Taylor, Z. W., & Bicak, I. (2021). Two-Year Institution and Community College Web Accessibility: Updating the Literature After the 2018 Section 508 amendment. In *Graduate Students' Research about Community Colleges* (pp. 125–135). Routledge. https://doi.org/10.4324/9781003011392-10

Teh, Y. F., & Ramli, S. N. (2023). Implementation of Multi-Factor Authentication on A Vaccination Record System. *Applied Information Technology and Computer Science*, *4*(1), 19–39. https://doi.org/10.30880/aitcs.2023.04.01.002

Thompson, K. M., & Copeland, C. (2020). Inclusive Considerations for Optimal Online Learning in Times of Disasters and Crises. *Information and Learning Sciences*, *121*(7/8), 481–486. https://doi.org/10.1108/ils-04-2020-0083

van Rensburg, M. J., Weaver, C., Jenkins, C., Banister, M., King, E., & Bell, S. (2020). Using an Advocacy Practicum to Establish a Framework for Virtual Community Consultations in the Ottawa Adult Autism Community. In *Transforming Social Work Field Education* (p. 227). https://doi.org/10.2307/j.ctv3405pqj.18

Vickers, W., Reddivari, S., & Reddivari, K. (2022, August). Evaluating Audio-to-Text utilizing Dragon in the Context of Just-in-Time Requirements. In *2022 IEEE 23rd International Conference on Information Reuse and Integration for Data Science (IRI)* (pp. 124–125). IEEE. https://doi.org/10.1109/iri54793.2022.00037

Willmore, B. D., & King, A. J. (2023). Adaptation in Auditory Processing. *Physiological Reviews*, *103*(2), 1025–1058. https://doi.org/10.1152/physrev.00011.2022

Zhang, S., & Balog, K. (2020). Web Table Extraction, Retrieval, and Augmentation: A Survey. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *11*(2), 1–35. https://doi.org/10.1145/3372117

Zubala, A., Kennell, N., & Hackett, S. (2021). Art Therapy in the Digital World: An Integrative Review of Current Practice and Future Directions. *Frontiers in Psychology*, *12*, 595536. https://doi.org/10.3389/fpsyg.2021.600070

Žuliček, L., Tomić, S., & Bosnić, I. (2021, September). Adapting Modularized Web Applications to Web Accessibility Standards. In *2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 470–475). IEEE. https://doi.org/10.23919/mipro52101.2021.9596750

Authors information

James Hutson – PhD, Head of the Department, Lead XR Disruptor, Lindenwood University
Address: 209 S. Kingshighway St, MO 63301, Saint Charles, United States
E-mail: jhutson@lindenwood.edu
ORCID ID: https://orcid.org/0000-0002-0578-6052

Piper Hutson – EdD, Lecturer, Lindenwood University
Address: 209 S. Kingshighway St, MO 63301, Saint Charles, United States
E-mail: phutson@lindenwood.edu
ORCID ID: https://orcid.org/0000-0002-1787-6143

Authors' contributions

James Hutson drafted the manuscript and critically revised it with valuable intellectual comments; developed the methodology design; conducted comparative analysis; collected literature; analyzed the United States legislation; drafted and edited the article; formulated the key findings, suggestions, and recommendations; and drafted the manuscript.
Piper Hutson formulated the idea, research objectives, and goals; participated in the research design; reviewed and summarized literature; analyzed the United States legislation; interpreted the specific and general research findings; critically reviewed and edited the manuscript; approved the final version of the article.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
ASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – August 10, 2023
Date of approval – September 20, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:349.3:364.23
EDN: https://elibrary.ru/aoqmxu
DOI: https://doi.org/10.21202/jdtl.2023.37

Цифровая инклюзия для людей с расстройствами аутистического спектра: пересмотр существующих правовых моделей и доктринальных концепций

Джеймс Хатсон ✉

Университет Линденвуд
г. Сент-Чарльз, США

Пайпер Хатсон

Университет Линденвуд
г. Сент-Чарльз, США

Ключевые слова

аутизм,
доступная среда,
законодательство,
инвалидность,
право,
расстройство аутистического спектра,
социальное обеспечение,
цифровая доступность,
цифровая инклюзия (инклюзивность),
цифровые технологии

Аннотация

Цель: в современном мире значительная доля профессиональных задач выполняется в цифровой среде, на цифровых площадках, в виртуальных и прочих собраниях, что обусловливает необходимость критического осмысления традиционных взглядов на проблему доступной среды и цифровой доступности с учетом базовых общечеловеческих потребностей инвалидов.

Методы: разрыв между традиционной правовой точкой зрения на особые условия труда для инвалидов и насущными потребностями «цифрового рабочего места» (цифровой среды) ярко показывает пробелы в понимании концепции доступности, которые выявляются и исследуются посредством формально-юридического и доктринального методов. Многогранные аспекты цифровой инклюзии раскрываются на основе информационного подхода к законодательству, который приводит в том числе к необходимости поиска имеющихся рекомендаций, направленных на заполнение указанного пробела и способствующих созданию более инклюзивной и ответственной правовой, общественной и технологической среды.

✉ Контактное лицо

Результаты: исследование темы привело к выводу о необходимости переоценки существующих правовых, общественных и технологических парадигм. Эта переоценка должна быть нацелена на выработку более инклюзивной и доброжелательной концепции доступной среды, которая учитывала бы разнообразие человеческого опыта и потребностей, широкий спектр поведенческих и когнитивных особенностей. Создание особых условий на рабочем месте для лиц с явными и скрытыми проблемами со здоровьем для работодателя должно стать неотъемлемой частью его внимания наряду с вопросами повышения эффективности управления.

Научная новизна: неявные (скрытые) проблемы со здоровьем традиционно не изучаются в должной мере, хотя они охватывают целый спектр психических и физических нарушений, которые, как и явные проблемы со здоровьем, различаются по своему происхождению, интенсивности, постоянному или эпизодическому характеру. Данное исследование восполняет пробел в части поиска ответов на вопросы об инвалидности и ее правовой защите с учетом тренда цифровой инклюзивности, динамического характера современной трудовой деятельности и широкого спектра способностей и потребностей людей.

Практическая значимость: рассматриваемые в исследовании аспекты скрытой или латентной инвалидности позволяют взглянуть на проблему занятости с иной точки зрения, обращая особое внимание на условия, которые можно было бы создать на рабочих местах. Работодатели чаще всего могут не осознавать необходимости создания особых условий труда лицам со скрытыми проблемами со здоровьем, в результате чего увеличивается безработица, растет число больничных; ограничиваются возможности на рабочем месте и многое другое. Сотрудники часто не стремятся по своему желанию раскрывать работодателям информацию о своих неочевидных проблемах со здоровьем, поэтому работодатели должны содействовать раскрытию такой информации, создавая необходимые условия для этого. Такой подход будет способствовать правовой защите данной категории работников и дальнейшему развитию существующего законодательного регулирования, которое не вполне отвечает современным потребностям и изменившейся реальности.

Для цитирования

Хатсон, Дж., Хатсон, П. (2023). Цифровая инклюзия для людей с расстройствами аутистического спектра: пересмотр существующих правовых моделей и доктринальных концепций. *Journal of Digital Technologies and Law*, *1*(4), 851–879. https://doi.org/10.21202/jdtl.2023.37

Список литературы

Baptista, J., Stein, M. K., Klein, S., Watson-Manheim, M. B., & Lee, J. (2020). Digital Work and Organisational Transformation: Emergent Digital/Human Work Configurations in Modern Organisations. *The Journal of Strategic Information Systems*, *29*(2), 101618. https://doi.org/10.1016/j.jsis.2020.101618

Blanco, M., Zong, J., & Satyanarayan, A. (2022). *Olli: An Extensible Visualization Library for Screen Reader Accessibility*. https://vis.mit.edu/pubs/olli.pdf

Bosio, E., Djankov, S., Glaeser, E., & Shleifer, A. (2022). Public Procurement in Law and Practice. *American Economic Review*, *112*(4), 1091–1117. https://doi.org/10.1257/aer.20200738

Brooks, A. (2017). Accessibility: Definition, Labeling, and CVAA Impact. *Recent Advances in Technologies for Inclusive Well-Being: From Worn to Off-body Sensing, Virtual Worlds, and Games for Serious Applications*, 283–383. https://doi.org/10.1007/978-3-319-49879-9_14

Burks, C. L. (2013). Improving Access to Commercial Websites Under the Americans with Disabilities Act and the Twenty-First Century Communications and Video Accessibility Act. *Iowa Law Review, 99*(1), 363. https://clck.ru/36kuL4

Caldwell, B., Cooper, M., Reid, L. G., Vanderheiden, G., Chisholm, W., Slatin, J., & White, J. (2008). *Web Content Accessibility Guidelines (WCAG) 2.0. WWW Consortium (W3C)*, *290*, 1–34. https://clck.ru/36kuNe

Capuano, A. (2022). Post-Pandemic Workplace Design and the Plight of Employees with Invisible Disabilities: In Australian Labour Law and Anti-Discrimination Legislation Equipped to Address New and Emerging Workplace Inequalities?. *The University of New South Wales Law Journal*, *45*(2), 873–913. https://doi.org/10.53637/emwr6179

Chiou, P. T., Alotaibi, A. S., & Halfond, W. G. (2021, August). Detecting and Localizing Keyboard Accessibility Failures in Web Applications. In *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (pp. 855–867). https://doi.org/10.1145/3468264.3468581

Clouse, J. R., Wood-Nartker, J., & Rice, F. A. (2020). Designing Beyond the Americans with Disabilities Act (ADA): Creating an Autism-Friendly Vocational Center. *HERD: Health Environments Research & Design Journal*, *13*(3), 215–229. https://doi.org/10.1177/1937586719888502

de Melo, F. D. A. F., Soares, K. P., de Barros, E. M., dos Santos Cabral, E. L., da Costa Júnior, J. F., da Silva, A. A. R. S., & Burlamaqui, A. M. F. (2022). Inclusive Digital Technologies in the Classroom: A Case Study Focused on Students with Autism Spectrum Disorder (ASD) in the Final Years of Elementary School. *Research, Society and Development*, *11*(6), e10211628759-e10211628759. https://doi.org/10.33448/rsd-v11i6.28759

Duarte, C., & Fonseca, M. J. (2019). *Multimedia Accessibility. In Web Accessibility: A Foundation for Research* (pp. 461–475). Springer, London. https://doi.org/10.1007/978-1-4471-7440-0_25

Farbenblum, B., & Berg, L. (2017). Migrant Workers' Access to Remedy for Exploitation in Australia: The Role of the National Fair Work Ombudsman. *Australian Journal of Human Rights*, *23*(3), 310–331. https://doi.org/10.1080/1323238x.2017.1392478

Fayyaz, N., & Khusro, S. (2023). Enhancing Accessibility for the Blind and Visually Impaired: Presenting Semantic Information in PDF Tables. *Journal of King Saud University – Computer and Information Sciences*, 101617. https://doi.org/10.1016/j.jksuci.2023.101617

Ferlazzo, E., Sueri, C., Masnou, P., Aguglia, U., Mercuri, S., Caminiti, E., & Piccioli, M. (2021). Technical Issues for Video Game Developers and Architects to Prevent Photosensitivity. In *The Importance of Photosensitivity for Epilepsy* (pp. 407–412). Springer, Cham. https://doi.org/10.1007/978-3-319-05080-5_33

Frey, B. A., & Mancilla, R. (2023). Inclusive Online Learning: Digital Accessibility Practices. In *Diversity in Higher Education Remote Learning: A Practical Guide* (pp. 93–104). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-31214-4_8

Gleason, C., Pavel, A., McCamey, E., Low, C., Carrington, P., Kitani, K. M., & Bigham, J. P. (2020, April). Twitter A11y: A Browser Extension to Make Twitter Images Accessible. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–12). https://doi.org/10.1145/3313831.3376728

Griffen, B., Woods-Catterlin, L., Lorah, E. R., & Whitby, P. S. (2022). Teaching Communication to Individuals with Autism Spectrum Disorders. In *Autism Spectrum Disorders: Advancing Positive Practices in Education.* (5th Ed.). Routledge. https://doi.org/10.4324/9781003255147-9

Hawkins, D. S. (2023). Overlooked and Undercounted: Communication and Police Brutality Against People with Disabilities. In *The Palgrave Handbook of Disability and Communication* (pp. 385–399). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-14447-9_23

Higgins, J. M., Arnold, S. R., Weise, J., Pellicano, E., & Trollor, J. N. (2021). Defining Autistic Burnout Through Experts by Lived Experience: Grounded Delphi Method Investigating #AutisticBurnout. *Autism*, *25*(8), 2356–2369. https://doi.org/10.1177/13623613211019858

Hodges, H., Fealko, C., & Soares, N. (2020). Autism Spectrum Disorder: Definition, Epidemiology, Causes, and Clinical Evaluation. *Translational Pediatrics*, *9*(Suppl 1), S55. https://doi.org/10.21037/tp.2019.09.09

Hurley-Hanson, A. E., Giannantonio, C. M., Griffiths, A. J., Hurley-Hanson, A. E., Giannantonio, C. M., & Griffiths, A. J. (2020). The Stigma of Autism. *Autism in the Workplace: Creating Positive Employment and Career Outcomes for Generation A* (pp. 21–45). https://doi.org/10.1007/978-3-030-29049-8_2

Hutson, P., & Hutson, J. (2023). Neurodiversity and Inclusivity in the Workplace: Biopsychosocial Interventions for Promoting Competitive Advantage. *Journal of Organizational Psychology*, *23*(2), 1–16. https://doi.org/10.33423/jop.v23i2.6159

Inal, Y., Guribye, F., Rajanen, D., Rajanen, M., & Rost, M. (2020, October). Perspectives and practices of digital accessibility: A survey of user experience professionals in Nordic countries. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (pp. 1–11). https://doi.org/10.1145/3419249.3420119

Maruthy, S., & Kelkar, P. (Eds.). (2023). *Understanding and Managing Fluency Disorders: From Theory to Practice*. Routledge. https://doi.org/10.4324/9781003367673

Jaeger, P. T. (2008). User-Centered Policy Evaluations of Section 508 of the Rehabilitation Act: Evaluating E-Government Web Sites for Accessibility for Persons with Disabilities. *Journal of Disability Policy Studies*, *19*(1), 24–33. https://doi.org/10.1177/1044207308315274

Kausar, S., Tahir, B., & Mehmood, M. A. (2021, December). HashCat: A Novel Approach for the Topic Classification of Multilingual Twitter Trends. In *2021 International Conference on Frontiers of Information Technology (FIT)* (pp. 212–217). IEEE. https://doi.org/10.1109/fit53504.2021.00047

Kharismadewi, Y., Revita, I., & AS, R. M. (2023). A Praat-Based Stuttering Analysis of the Main Character in the King's Speech Movie: A Neuropsycholinguistic Study. *Journal of Applied Studies in Language*, *7*(1), 56–65. https://doi.org/10.31940/jasl.v7i1.56-65

Kous, K., Kuhar, S., Pavlinek, M., Heričko, M., & Pušnik, M. (2021). Web Accessibility Investigation of Slovenian Municipalities' Websites Before and After the Adoption of European Standard EN 301 549. *Universal Access in the Information Society*, *20*, 595–615. https://doi.org/10.1007/s10209-020-00732-9

Kous, K., Kuhar, S., Rajšp, A., & Šumak, B. (2020, September). Investigation of the Accessibility of Non-Text Content Published on Websites. In *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 1645–1650). IEEE. https://doi.org/10.23919/mipro48935.2020.9245288

Krogh, K., & Johnson, J. (2006). A Life without Living: Challenging Medical and Economic Reductionism in Home Support Policy for People with Disabilities. In *D. Pothier, & R. Devlin (Eds.), Critical disability theory: Essays in philosophy, politics, policy and law* (pp. 151–176). Vancouver: University of British Columbia Press. https://doi.org/10.59962/9780774851695-010

Lister, K., Coughlan, T., Iniesto, F., Freear, N., & Devine, P. (2020, April). Accessible Conversational User Interfaces: Considerations for Design. In *Proceedings of the 17th International Web for All Conference* (pp. 1–11). https://doi.org/10.1145/3371300.3383343

Lowndes, A. M., & Connelly, D. M. (2023). User Experiences of Older Adults Navigating an Online Database of Community-Based Physical Activity Programs. *Digital Health*, *9*. https://doi.org/10.1177/20552076231167004

Matthews, C. K., & Harrington, N. G. (2000). Invisible disabilities. In *D.O. Braithwaite, & T. L. Thompson (Eds.), Handbook of Communication and People with Disabilities: Research and Application* (pp. 405–421). New Jersey: Lawrence Erlbaum Associates, Inc.

McCauley, J. B., Pickles, A., Huerta, M., & Lord, C. (2020). Defining Positive Outcomes in More and Less Cognitively Able Autistic Adults. *Autism Research*, *13*(9), 1548–1560. https://doi.org/10.1002/aur.2359

McKee, E., Popiel, M., & Boyce, W. (2006). *Policies and Programs to Facilitate Labour Force Participation for People with Episodic Disabilities: Recommendations for a Canadian Context Based on an International Analysis*. Toronto: Canadian Working Group on HIV and Rehabilitation.

Michelsanti, D., Tan, Z. H., Zhang, S. X., Xu, Y., Yu, M., Yu, D., & Jensen, J. (2021). An Overview of Deep-Learning-Based Audio-Visual Speech Enhancement and Separation. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, *29*, 1368–1396. https://doi.org/10.1109/taslp.2021.3066303

Mollow, A. (2010). When Black Women Start Going on Prozac. In *L. J. Davis (Ed). The Disability Studies Reader* (3d Ed., pp. 486–506). New York: Routledge.

Morgan, J. N. (2021). Policing Under Disability Law. *Stanford Law Review*, *73*, 1401–1469.

Mostafa, M. (2014). Architecture for Autism: Autism ASPECTSS™ in School Design. *International Journal of Architectural Research: ArchNet-IJAR*, *8*(1), 143–158. https://doi.org/10.26687/archnet-ijar.v8i1.314

Murphy, K. L. (2020). Civil Rights Laws: Americans With Disabilities Act of 1990 and Section 504 of the Rehabilitation Act of 1973. *Journal of Physical Education, Recreation & Dance*, *92*(1), 57–59. https://doi.org/10.1080/07303084.2021.1844555

Nath, H. K., & Liu, L. (2017). Information and Communications Technology (ICT) and Services Trade. *Information Economics and Policy*, *41*, 81–87. https://doi.org/10.1016/j.infoecopol.2017.06.003

Neely, B. H., & Hunter, S. T. (2014). In a Discussion on Invisible Disabilities, Let Us Not Lose Sight of Employees on the Autism Spectrum. *Industrial and Organizational Psychology*, *7*(2), 274–277. https://doi.org/10.1111/iops.12148

Olalere, A., & Lazar, J. (2011). Accessibility of US Federal Government Home Pages: Section 508 Compliance and Site Accessibility Statements. *Government Information Quarterly*, *28*(3), 303–309. https://doi.org/10.1016/j.giq.2011.02.002

Panda, S., & Chakravarty, R. (2020). Evaluating the Web Accessibility of IIT Libraries: A Study of Web Content Accessibility Guidelines. *Performance Measurement and Metrics*, *21*(3), 121–145. https://doi.org/10.1108/pmm-02-2020-0011

Patton, E. (2022). To Disclose or Not Disclose a Workplace Disability to Coworkers: Attributions and Invisible Health Conditions in the Workplace. *Equality, Diversity and Inclusion: An International Journal*, *41*(8), 1154–1180. https://doi.org/10.1108/edi-09-2021-0228

Pham, M., Singh, K., & Jahnke, I. (2023). Socio-Technical-Pedagogical Usability of Online Courses for Older Adult Learners. *Interactive Learning Environments*, *31*(5), 2855–2871. https://doi.org/10.1080/10494820.2021.1912784

Prince, M. J. (2017). Persons with Invisible Disabilities and Workplace Accommodation: Findings from a Scoping Literature Review. *Journal of Vocational Rehabilitation*, *46*(1), 75–86. https://doi.org/10.3233/jvr-160844

Proença, M. D. Q., Motti, V. G., Rodrigues, K. R. D. H., & Neris, V. P. D. A. (2021). Coping with Diversity-A System for End-users to Customize Web User Interfaces. *Proceedings of the ACM on Human-Computer Interaction*, *5*(EICS), 1–27. https://doi.org/10.1145/3457151

Reeve, T., & Gottselig, S. (2011). *Investigating Workplace Accommodation for People with Invisible Disabilities, Research Report*. Vancouver: BC Coalition of People with Disabilities.

Schall, C. M. (1998). The Americans with Disabilities Act – are we keeping our promise? An analysis of the effect of the ADA on the employment of persons with disabilities. *Journal of Vocational Rehabilitation*, *10*(3), 191–203. https://doi.org/10.3233/jvr-1998-10303

Schoen, J. (2022). Patching Procedural Potholes in Supplemental Jurisdiction Claims Involving ADA & Unruh Act Litigation in California Federal Courts. *Loyola Law Review*, *55*(4), 1107–1132. https://clck.ru/36kuXG

Seo, K., Dodson, S., Harandi, N. M., Roberson, N., Fels, S., & Roll, I. (2021). Active Learning with Online Video: The Impact of Learning Context on Engagement. *Computers & Education*, *165*, 104132. https://doi.org/10.1016/j.compedu.2021.104132

Shriberg, L. D., Kwiatkowski, J., & Mabie, H. L. (2019). Estimates of the Prevalence of Motor Speech Disorders in Children with Idiopathic Speech Delay. *Clinical Linguistics & Phonetics*, *33*(8), 679–706. https://doi.org/10.1080/02699206.2019.1595731

Smith, I. C., & White, S. W. (2020). Socio-Emotional Determinants of Depressive Symptoms in Adolescents and Adults with Autism Spectrum Disorder: A Systematic Review. *Autism*, *24*(4), 995–1010. https://doi.org/10.1177/1362361320908101

Taylor, Z. W., & Bicak, I. (2021). Two-Year Institution and Community College Web Accessibility: Updating the Literature After the 2018 Section 508 amendment. In *Graduate Students' Research about Community Colleges* (pp. 125–135). Routledge. https://doi.org/10.4324/9781003011392-10

Teh, Y. F., & Ramli, S. N. (2023). Implementation of Multi-Factor Authentication on A Vaccination Record System. *Applied Information Technology and Computer Science*, *4*(1), 19–39. https://doi.org/10.30880/aitcs.2023.04.01.002

Thompson, K. M., & Copeland, C. (2020). Inclusive Considerations for Optimal Online Learning in Times of Disasters and Crises. *Information and Learning Sciences*, *121*(7/8), 481–486. https://doi.org/10.1108/ils-04-2020-0083

van Rensburg, M. J., Weaver, C., Jenkins, C., Banister, M., King, E., & Bell, S. (2020). Using an Advocacy Practicum to Establish a Framework for Virtual Community Consultations in the Ottawa Adult Autism Community. In *Transforming Social Work Field Education* (p. 227). https://doi.org/10.2307/j.ctv3405pqj.18

Vickers, W., Reddivari, S., & Reddivari, K. (2022, August). Evaluating Audio-to-Text utilizing Dragon in the Context of Just-in-Time Requirements. In *2022 IEEE 23rd International Conference on Information Reuse and Integration for Data Science (IRI)* (pp. 124–125). IEEE. https://doi.org/10.1109/iri54793.2022.00037

Willmore, B. D., & King, A. J. (2023). Adaptation in Auditory Processing. *Physiological Reviews*, *103*(2), 1025–1058. https://doi.org/10.1152/physrev.00011.2022

Zhang, S., & Balog, K. (2020). Web Table Extraction, Retrieval, and Augmentation: A Survey. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *11*(2), 1–35. https://doi.org/10.1145/3372117

Zubala, A., Kennell, N., & Hackett, S. (2021). Art Therapy in the Digital World: An Integrative Review of Current Practice and Future Directions. *Frontiers in Psychology*, *12*, 595536. https://doi.org/10.3389/fpsyg.2021.600070

Žuliček, L., Tomić, S., & Bosnić, I. (2021, September). Adapting Modularized Web Applications to Web Accessibility Standards. In *2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 470–475). IEEE. https://doi.org/10.23919/mipro52101.2021.9596750

Сведения об авторах

Хатсон Джеймс – PhD, заведующий кафедрой, ведущий специалист в области дополненной реальности, Университет Линденвуд
Адрес: МО 63301, США, г. Сент-Чарльз, ул. С. Кингшайвей, 209
E-mail: jhutson@lindenwood.edu
ORCID ID: https://orcid.org/0000-0002-0578-6052

Хатсон Пайпер – доктор педагогики, преподаватель, Университет Линденвуд
Адрес: МО 63301, США, г. Сент-Чарльз, ул. С. Кингшайвей, 209
E-mail: phutson@lindenwood.edu
ORCID ID: https://orcid.org/0000-0002-1787-6143

Вклад авторов

Джеймс Хатсон осуществлял составление черновика рукописи и его критический пересмотр с внесением ценных замечаний интеллектуального содержания; разработку дизайна методологии; проведение сравнительного анализа; сбор литературы; анализ законодательства Соединенных Штатов Америки; подготовку и редактирование текста статьи; формулировку ключевых выводов, предложений и рекомендаций; оформление рукописи.
Пайпер Хатсон осуществляла формулирование идеи, исследовательских целей и задач; участие в научном дизайне; анализ и обобщение литературы; анализ законодательства Соединенных Штатов Америки; интерпретацию частных результатов исследования; критический пересмотр и редактирование текста рукописи; интерпретацию общих результатов исследования; утверждение окончательного варианта статьи.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.67.91 / Право социального обеспечения в отдельных странах
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 10 августа 2023 г.
Дата одобрения после рецензирования – 20 сентября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.38

Towards Legal Regulations of Generative AI in the Creative Industry

Natalia I. Shumakova ✉

Law Institute, South Ural State University (national research university)
Chelyabinsk, Russia

Jordan J. Lloyd

Unseen History
Essex, United Kingdom

Elena V. Titova

Law Institute, South Ural State University (national research university)
Chelyabinsk, Russia

Keywords

artificial intelligence,
copyright law,
creative industry,
digital technologies,
generative artificial intelligence,
intellectual property,
international law,
neural network,
object of copyright law,
subject of copyright law

Abstract

Objective: this article aims to answer the following questions: 1. Can generative artificial intelligence be a subject of copyright law? 2. What risks the unregulated use of generative artificial intelligence systems can cause? 3. What legal gaps should be filled in to minimize such risks?

Methods: comparative legal analysis, sociological method, concrete sociological method, quantitative data analysis, qualitative data analysis, statistical analysis, case study, induction, deduction.

Results: the authors identified several risks of the unregulated usage of generative artificial intelligence in the creative industry, among which are: violation of copyright and labor law, violation of consumers rights and the rise of public distrust in government. They suggest that a prompt development of new legal norms can minimize these risks. In conclusion, the article constants that states have already begun to realize that the negative impact of generative artificial intelligence on the creative industry must not be ignored, hence the development of similar legal regulations in states with completely different regimes.

✉ Corresponding author

Scientific novelty: the article provides a comprehensive study of the impact of generative artificial intelligence on the creative industry from two perspectives: the perspective of law and the perspective of the industry. The empirical basis of it consists of two international surveys and an expert opinion of a representative of the industry. This approach allowed the authors to improve the objectivity of their research and to obtain results that can be used for finding a practical solution for the identified risks. The problem of the ongoing development and popularization of generative artificial intelligence systems goes beyond the question "who is the author?" therefore, it needs to be solved by introduction of other than the already existing mechanisms and regulations – this point of view is supported not only by the results of the surveys but also by the analysis of current lawsuits against developers of generative artificial intelligence systems.

Practical significance: the obtained results can be used to fasten the development of universal legal rules, regulations, instruments and standards, the current lack of which poses a threat not only to human rights, but also to several sectors within the creative industry and beyond.

For citation

Shumakova, N. I., Lloyd, J. J., & Titova, E. V. (2023). Towards Legal Regulations of Generative AI in the Creative Industry. *Journal of Digital Technologies and Law, 1*(4), 880–908. https://doi.org/10.21202/jdtl.2023.38

Content

Introduction

In the year 2023, even those who never showed interest in the development of generative AI systems have encountered with the results of their negative impact on the creative industry due to the strike of The Screen Actors Guild-American Federation of Television and Radio Artists (the SAG-AFTRA) and the Writers Guild of America (the WGA) strike, which have

already resulted into delay of releases of highly-anticipated products[1] and, allegedly, can change the entire industry in the foreseeable future[2].

It is safe to say that the named strikes have influenced the academic and legal view on the use of generative AI: from the attempts to establish whether generative AI can be seen as a creator and how to protect AI-generated outputs (Wan & Lu, 2021) they have switched to the study of its impact on artists livelihoods (Sparkes, 2022) and discussion of requirements to responsible generative AI systems (Díaz-Rodríguez et al., 2023).

Taking into account the results of previous research works, the authors of this article identified the need of conducting a comprehensive analysis of possible risk connected to the unregulated use of generative AI. In order to reveal whether it is actually an existential threat[3] to the creative industry, they employed a number of multidisciplinary methods, conducted two surveys on ethics of the use generative AI in the creative and cultural industries, and invited a representative of the creative industry to provide an opinion on the subject where needed. Hence, the title of this article.

The article is separated in two chapters "The voice of law" and "The voice of the industry" and includes results of the conducted surveys, statistics, results of comparative legal analysis and case study etc.

In conclusion, the authors state that despite the current lack of international legal regulations of the usage of generative AI systems in the creative industry, states have already been coming up with fairly similar law projects the final goal of which is to increase the accountability of companies that produce and/or own generative AI systems, the key here is to adopt and enforce such regulations promptly in order to reduce the identified risks and prevent possible harm.

1. The voice of law

The attempts to invent a robot that would be able to create something aren't new. In fact, the first robots that were imitating the creative process were introduced over 500 years ago and it immediately raised the question about whether or not they could replace actual human beings[4]. In the 18th century, they became known as "automatons" and gained an enormous popularity – this is when Jaquet Droz produced his famous automatons that were drawing pictures, playing musical instruments and entertaining

1 Kelley, S. (2023, September 19). All the major movies and TV shows delayed by the strikes. Los Angeles Times. https://clck.ru/36n37w

2 Belloni, M., & Shaw, L. (2023, September 18). The Strike's Permanent Damage: Who Will Suffer the Most? The Ringer. https://clck.ru/36n38d

3 We're Fighting for the Survival of Our Profession. SAG-AFTRA Strike. https://clck.ru/36n39G

4 Marvellous machines: early robots. (2018, November 20). Science Museum. https://goo.su/Scuk

public in other ways by doing that they were programmed to do[5]. It would be fair to say that generative AI systems function more or less similar to those early robots – they do that they were programmed to do by employing various techniques to generate a product based on the data used to train them. And yet for years scholars have been asking the question not that different than 3 centuries ago – "Can generative AI be a creator?" (Somenkov, 2019). Usually, this question is immediately followed up by another one – "Can products of generative AI be an object of intellectual property rights and copyright law?" (Agibalova & Perekrestova, 2020). Responses to these questions vary. But this alone proves that the current legal status of generative AI systems is uncertain (Stokel-Walker, 2023). Here, we tend to support the opinion that questions about the relationship between humans and machines in the creative process and those about the shifting character of the network of relevant stakeholders implicated in this process are more important because responses to the others can be found in the existing legislature of most countries (Fenwick & Jurčys, 2023). Nevertheless, it's worth-mentioning that there are exclusions such as China and New Zealand. Should we take a look at Chinese lawsuits and court resolutions, we might notice that this country tends to practice a mixed approach towards the recognition of an object of copyright law – Y. Wan and H. Lu in their research work provides two examples of it: 1) Beijing Film Law Firm vs. Beijing Baidu Netcom Science & Technology Co Ltd, where the Beijing Internet Court concluded the object of the dispute was completely generated by AI and therefore, could not be protected by copyright; 2) Shenzhen Tencent Computer System Co Ltd vs Shanghai Yingxun Technology Co Ltd, where the Nanshan District Court of Shenzhen analyzed the actions taken by an actual human in the process of generation the object of the dispute and ruled that the output of it was protectable under the Copyright Law of China (Wan & Lu, 2021). New Zealand, in their turn, has chosen a completely different approach – according to the section "Interpretation" of their Copyright Act (1994), "computer-generated, in relation to a work, means that the work is generated by computer in circumstances such that there is no human author of the work"[6], so theoretically, according to the logic of this norm, generative AI can be a subject of copyright and its products – objects of copyright law. However, Article 5 "Meaning of authorship" doesn't add it on the list of possible authors, more other, it says that "the author of a work is the person who creates it"[7], which again causes the uncertainly of generative AI's legal status.

In Russia, no special legal regulations for the use of generative AI in the creative industry have been developed yet, but for the goal of this research it is important to study recommendations and commentaries provided by legal advisors and lawyers in regards of the cooperate protection of generated products. Some of them insist that it's high time

5 DNA. Jaquet Droz. https://clck.ru/36nqDJ

6 Copyright Act 1994 No. 143. Version as at 31 May 2023. (2023). Parliamentary Council Office. https://clck.ru/36n3Ds

7 Ibid.

the country developed new mechanisms and institutions to put generative AI systems under control[8], whereas others consider the current legal norms being enough to respond to the new challenges associated with the development of the named technologies and their usage[9]. Recommendations provided in open sources for businesses in regards of employing generative AI systems should also be a matter of our interest. For instance, Semyonov A. (IT Moscow Digital School) suggests that products generated by AI are not objects of copyright law and thus, can be freely use for commercial purposes[10]. Yu. Brisov (Digital & Analogue Partners) represents an opposite point of view and recommends to carefully study terms and conditions provided by creators of each of the generative AI systems because according to them, not users but owners or creators such a system can be subjects of copyright law and that applies not exclusively to the use of Russian generative AI systems[11]. And indeed, YandexArt, for instance, restricts any commercial use of images and texts generated with their system, moreover, according to their terms and conditions, products generated in the application "Shedevrum" can be used for commercial purposes by the company itself[12]. Oddly enough, in the press-release of the mentioned application, no such information is provided, furthermore, it creates quite the opposite impression[13].

Lawyers of the United States and the United Kingdom also tend to publically express their opinion on the matter. Joseph Saveri Law Firm on their official webpage claims that products generated with the use of Stable Diffusion, DreamStudio, DreamUp, and Midjourney "infringe on the rights of thousands of artists and creators" and cause nothing less than an actual "financial burden"[14]. This notion corresponds with the comments provided by D. Lee (BDB Pitmans), in which he highlights that even the lack of adequate terminology in case with the use of generative AI systems can be harmful, the lawyer also highlights that it can be "challenging to demonstrate tangible harm" due to the specifics of the training process of such systems, additionally, he suggests that the use of generative AI systems can violate the moral rights of human creators on whose works those systems were taught because "the AI's unauthorized use of their work might alter its meaning, potentially

8 Reshetnikova, A. (2019, October 29). A creator or a tool in the author's hamds? Advokatskaya Gazeta. https://clck.ru/36n3Ge

9 A brain twister: jurists' glance at artificial intelligence. (2023, April 20). Advokatskaya Gazeta. https://clck.ru/36n3HJ

10 Kildyushkin, R. (2022, July 13). It became known who owns copyright to images created by neural networks. Gazeta.ru. https://goo.su/ER4l

11 Brisov, Yu. (2023, May 25).May one use the creative works of neural networks in business? Bisnes Secrety. https://clck.ru/36n3KB

12 Terms of us of Shedevrum. Yandex. https://clck.ru/3663j8

13 YandexArt. Ya.ru. https://clck.ru/36n3L9

14 AI Image Generator – Copyright Litigation. Joseph Savery Law Firm. https://clck.ru/36n3LZ

damaging their reputation or the work's artistic value" (the right to object to the derogatory treatment of their work), then he adds, that under the current laws the use of copyright-protected material for training generative AI can be seen as "fair"[15].

A special say has the United States Copyright Office. According to their decision from February 21, 2023, AI-generated works cannot be a subject of copyright, furthermore, they rescinded the first original registration of a work generated with the use of Midjourney (Kristina Kashtanova's comic book) and recognized as object of copyrights law only its text and "selection, coordination, and arrangement of text created by the author", but not the generated images[16]. The UK Court of Appeal takes a similar to the US Copyright Office position – according to their recent decision, generative AI systems cannot be inventors and therefore their products cannot be considered objects of patent law[17].

The position of Australia towards the use of generative AI systems also cannot be ignored – the Albanese government, for example, considers generative AI systems an existential threat due to their ability to produce "deep-fakes", multiply disinformation and influence the democratic processes in other ways, hence the recent discussion of either banning or putting them under control[18]. Meanwhile, according to the recent survey conducted by BlackBerry Limited, 93 % of Australian companies are currently implementing or considering the implementation of bans on generative AI systems within the workplace because they see them as a threat to both security and reputation[19]. BlackBerry Limited in their research[20] also demonstrates that this trend is global and 75 % companies worldwide share the Australian point of view on these digital technologies despite admitting the fact that they could be a useful instrument.

In order to understand a possible negative impact of the use of generative AI systems, two of the House of Common's committees conducted comprehensive investigations, the results of which were reported earlier this year[21, 22]: both of the reports revealed a real possibility of violation of copyrights, intellectual property rights, labor rights and the threat

---

15 AI authors – what a US lawsuit could mean for UK IP law. (2023, August 10). The Trademark Lawyer. https://clck.ru/36n3PR

16 Re: Zarya of the Dawn (Registration # VAu001480196). (2023, February 21). United States Copyright Office. https://clck.ru/36n3Pk

17 Neutral Citation Number: [2021] EWCA Civ 1374 Case No: A3/2020/1851. British and Irish Legal Information Institute. https://clck.ru/36n3Qb

18 Safe and responsible AI. (2023, June 1). Ministry for Industry and Science. https://goo.su/rs4z

19 Organisations in Australia set to ban ChatGPT and generative AI apps on work devices. APDR – Asia-Pasific Defense Reporter. (2023, August 14). https://clck.ru/36KzWP

20 Why Are So Many Organizations Banning ChatGPT? (2023, August 8). BlackBerry. https://clck.ru/36n3S4

21 UK Parliament. (2023). Connected tech: AI and creative technology: Eleventh Report of Session 2022–23. https://clck.ru/36n3Sf

22 UK Parliament. (2023). The governance of artificial intelligence: interim report: Ninth Report of Session 2022–23. https://clck.ru/36n3TN

of mass-production of disinformation, "deep-fakes" and other illegal content in case of the current legal gaps, including the abstractive terminology, will not be filled in the nearest future. All in all, the recommendations provided in the first report[23] correspond with recommendations of The UK Intellectual Property Office – the UK legislation needs to be change in order to be able to adequately response to the challenges causes by the development of digital technologies[24]. The results of the named investigations were used to formulate a list of social harms that can be caused by the on-going unregulated use of generative AI systems, among which are: degradation of information environment; labor market disruption; bias and representational harms[25].

Still and all, up to this day, China is the only country that has already regulated the use of generative AI systems, hence the importance of analyzing their approach. Article 7 of "The Interim Measures for Generative Artificial Intelligence Service Management", that came in force earlier this year, obliges to train generative AI systems only on ethically-sourced data in order to prevent any possible violation of copyrights or intellectual property rights, whereas Article 12 obliges providers of generative AI services to label their products as such[26]. Chinese lawyers clarify that according to the new rules, providers are also required to label data in the process of research and development[27], additionally, they prove that public commentaries on the draft of these measures were taken into account[28]. And in order to make the enforced regulations work, the National Information Security Standardization Technical Committee released "Network Security Standard Practice Guide—Generative Artificial Intelligence Service Content Identification Method" that in details provides information on how products of generative AI should be labelled, why it needs to be done[29]. Thus, the fair claim that China is the pioneer in legal regulations of the usage of generative AI systems.

2. The voice of the industry

The analysis of the current attempts to regulate the use of generative AI systems shows that the UK and China try to take into account the voice of the industries (both – the creative and the cyber ones) and consumers of their products. In fact, the voices of human creators

23 UK Parliament. (2023). Connected tech: AI and creative technology: Eleventh Report of Session 2022–23. https://clck.ru/36n3Sf

24 IPO Transformation programme: second consultation. (2023, August 22). GOV.UK. https://clck.ru/36n3zQ

25 AI safety summit. Department For Science, Innovation and Technology. https://clck.ru/36n3zq

26 生成式人工智能服务管理暂行办法 от 1994 № 143 // 国家互联网信息办公室. (2023). – 第15号 10.07.2023. https://goo.su/fbbG

27 Regulatory and legislation: China's Interim measures for the Management of Generative Artificial Intelligence Services officially implemented. (2023, August). 普华永道中国. https://clck.ru/36n43s

28 Cai, R., & Zhu, W. (2023, July 14). Comparative Analysis of China's New Generative AI Regulations. Zhong Lun. https://clck.ru/36n44e

29 网络安全标准实践指南—生成式人工智能服务内容标识方法 - 2023 № TC260-PG-20233A. (2023). 全国信息安全标准化技术委员会秘书处. https://goo.su/Gl6Shf1

have become so laud recently that even the Senate of the USA had to listen to them[30]. Lawsuits, congressional hearings and, of course, the strikes – all of these can be considered signs of a growing public, or to be more precise - political public distrust. And indeed, when nationals of a country feel uncertain about their future (Küçükkömürler & Özkan, 2022), feel that they have been "left behind" (Stroppe, 2023) or consider their government being unable to take appropriate legal actions in order to reduce the risks that those nationals see as an expectational threat, they tend to take actions such as strikes, protests and rallies (Torres & Bellinger, 2014). And certainly, it doesn't help the situation when media giants like Time release information about corporations like OpenAI lobbying their interests to "water down Europe's AI rules"[31] and succeeding in it[32]. Furthermore, it seems that usual negotiators, whose entire purpose of existence of which is to represent lawful interests of the creative industry, have been doing the exact opposite[33]. On top of that, leaders of opinions such as Alex Winter, also publicly express their political distrust, accusing the government of being "captured by BigTech" and calling The People's Summit[34] more essential than the AI Safety Summit[35], which, in their opinion, will only worsen the situation because for the governments "it's impossible to protect their citizens"[36]. Hence, the importance to study the opinion of the creative industry and consumers of its products, which, in this article are expressed in the results of two international surveys and provided by the co-author of it – Jordan J. Lloyd (*written in italics*).

The surveys were conducted on social media and Telegram from July 11 to October 11, 2023.

Geography and of the surveys:

103 of 117 the English-speaking responders provided information about their residency – according to the responses, they represent 21 countries such as: The US, The UK, Argentina, Canada, Belgium, Germany, France, Norway, Netherlands, Turkey, Denmark, South Africa, Chile, Czech Republic, Serbia, Australia, Austria, Italy, Ireland, New Zealand, Sweden (Fig. 1), whereas the absolute majority of them work in the creative/cultural industry – 85.5 %, and only 14.5 % of the English-speaking responders are consumers of its products (Fig. 2).

30 Artificial Intelligence and Intellectual Property – Part II: Copyright. Subcommittee on intellectual property. https://clck.ru/36n3aE

31 Big Tech Is Already Lobbying to Water Down Europe's AI Rules. Time. https://clck.ru/36n3ak

32 Exclusive: OpenAI Lobbied the E.U. to Water Down AI Regulation. Time. https://clck.ru/36n3bJ

33 We're Fighting for the Survival of Our Profession. SAG-AFTRA Strike. https://clck.ru/36n39G

34 The People's AI Summit – The citizens. YouTube. https://clck.ru/36n3cb

35 AI Safety Summit: introduction. GOV.UK. https://clck.ru/36n4AB

36 AI's threat to democracy and labour looms large. UK's 'doomsday' AI summit is poised to make things worse. Big Issue. https://clck.ru/36n3dx

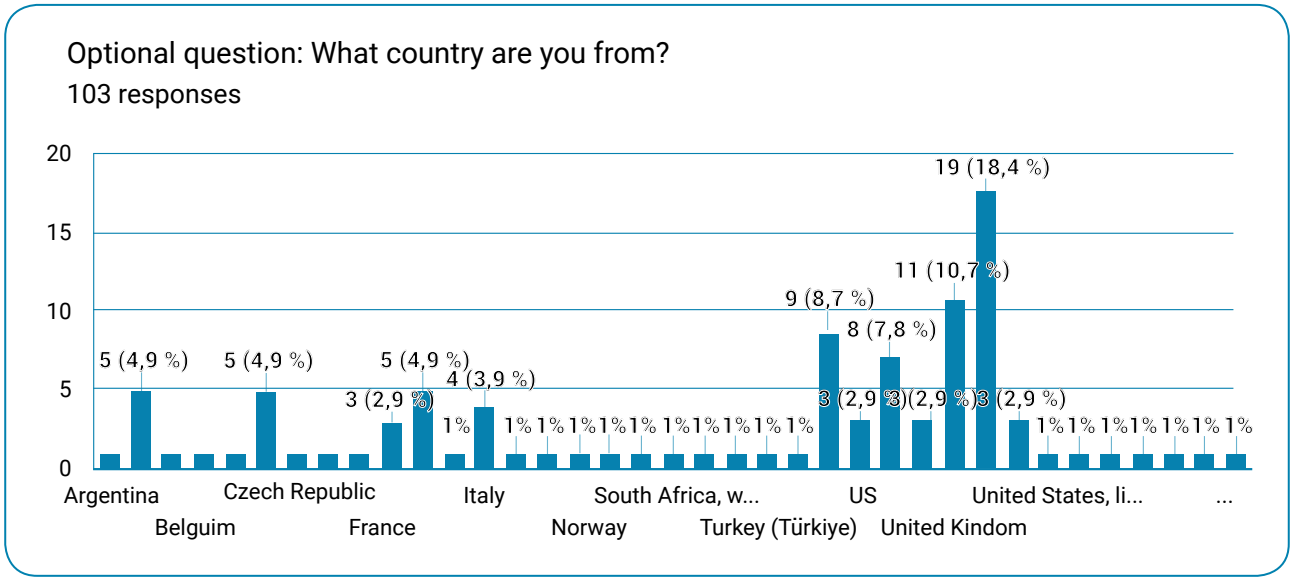


Fig. 1

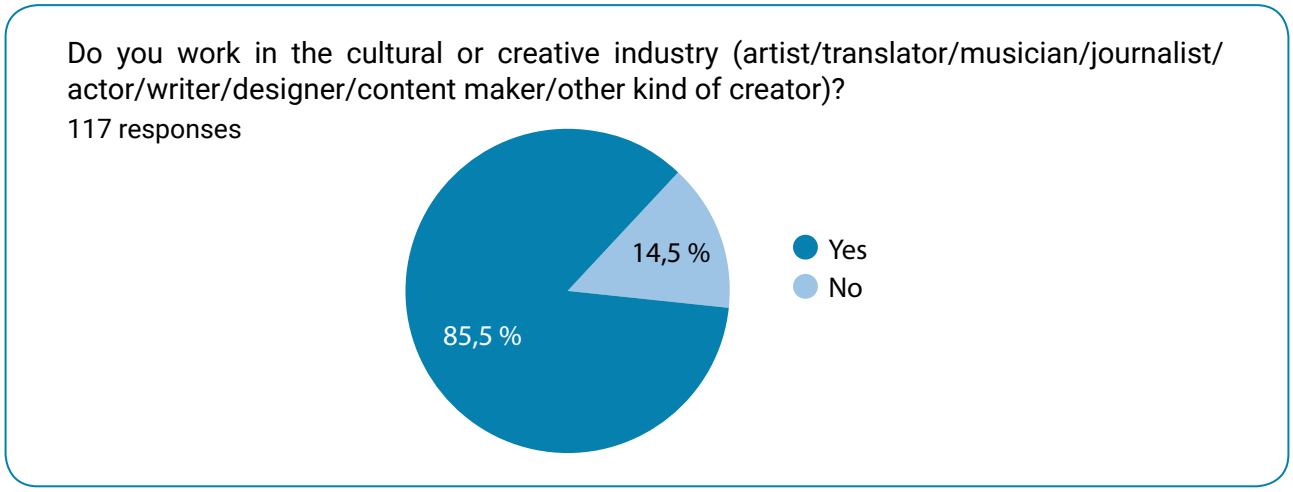


Fig. 2

31 of the 36 Russian-speaking responders also provided such an information and according to their answers, they represent 4 countries: Russia– 90.4 %, Moldova – 3.2 %, Poland – 3.2 % and Latvia – 3.2 %, and the absolute majority of them are involved in the creative industry too – 72.2 %, while 27.8 % of the Russian-speaking responders are consumers of their products.

Ethics of the surveys: the surveys were anonymous; all of the responders were informed about the possible use of their responses for academic purposes.

2.1. Generative AI as a subject of copyright law, products of generative AI as objects of copyright law

In the previous chapter, we established that neither academics nor law-makers don't have a universal understanding of whether we can consider generative AI a creator. Mr. Lloyd provided here his point of view, according to which, generative AI cannot be seen as such:

"*Copyright Law as written covers expressions created by human endeavour. As noted, the creation of prompts is based on human imagination, but the resulting process and generated asset is not, therefore cannot be copyrighted if we accept the prevailing mindset. I akin Generative AI to a form of gambling, like a slot machine at a casino. Spinning the reels creates variations, where you can lock in certain variations you like, then spin the reel again to achieve a more desirable result. This is, more or less, how prompters work when utilising Generative AI*". The question that always follows the discussion about the legal status of generative AI is whether we can protect products generated with the use of it as objects of copyright law and intellectual property rights. Again, as we established earlier, under the letter of law it is possible in several countries. But the question is – should we do it? "*No, or at least, it should have a new form of copyright / intellectual property (IP) protection framework to cover assets generated by AI as a distinctly separate entity from existing copyright law. The existing copyright framework is not perfect but it is well established, benefiting creators and IP businesses alike. The protections and reimbursements offered by the existing system are of course, under threat from the deluge of AI generated assets. I read somewhere that it took just nine months to generate as many 'new' artworks as there have been in the entirety of recorded history. Clearly, copyright and IP legislation will need to act fast in order to protect original creators*".

These questions were asked in the surveys and the results clearly indicated a view common within the creative industry and consumers of its products: 65 % of the English-speaking responders don't think that products of generative AI should be protected by copyright law (Fig. 3) and the same percentage don't consider that products of AI should be protected by intellectual property rights (Fig. 4), whereas 11.1 % think products generated with the use of AI should be protected by copyright law (Fig. 3) and 9.4 % suggest that such products should be protected by intellectual property rights (Fig. 4).

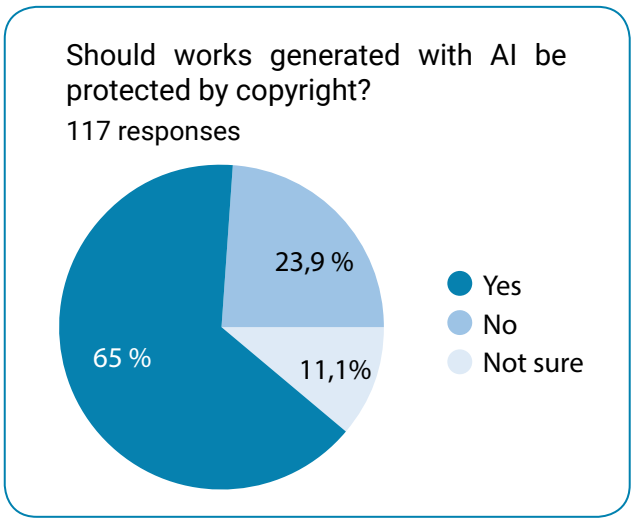


Fig. 3

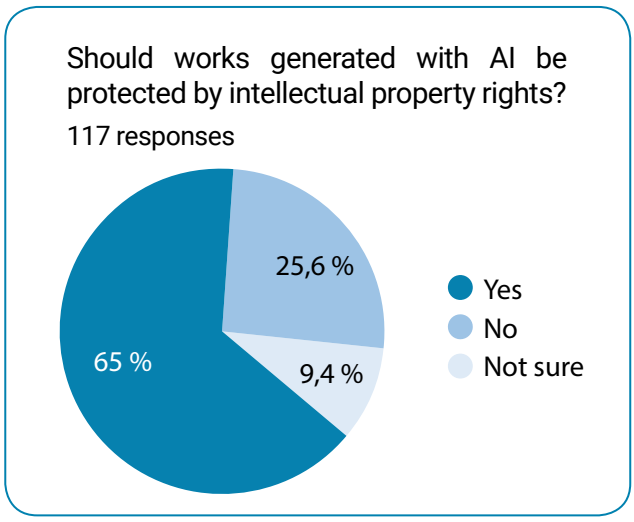


Fig. 4

The Russian-speaking responders answered to the same questions and 61.1% of them consider that such products should be protected neither with the copyright law (Fig. 5) nor by intellectual property rights (Fig. 6). However, 25 % of the Russian-speaking responders think that products of generative AI should be protect as objects of copyright law (Fig. 5) and the same percentage of them suggest that products of generative AI should be protected by intellectual property rights (Fig. 6).

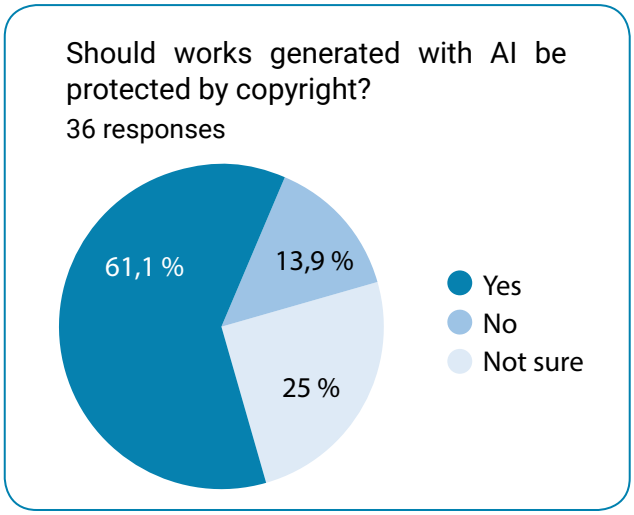


Fig. 5

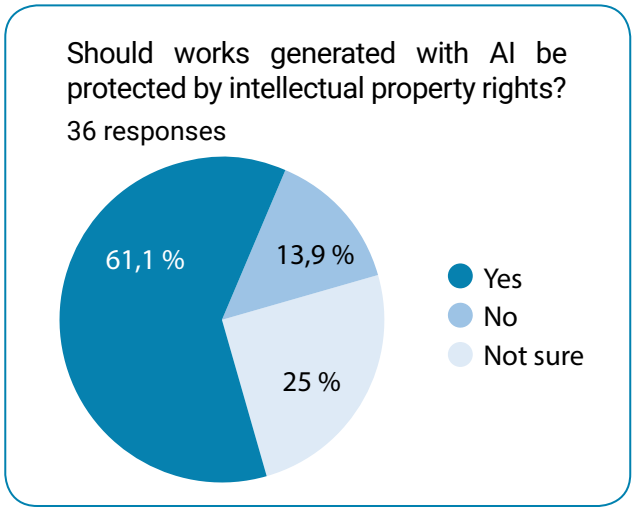


Fig. 6

Another question that is yet to be answered both by creators and consumers, do generated products have artistic and cultural value? And can they actually be valued as much as products of creative human expression? "*That's a very good question. For me the issue is that the average person will soon not be able to tell the difference between the two. Creative endeavours are subject to personal preference and opinion. For me, I am now far more interested in the process of creation and the addition of context and human imagination when I engage with a piece of work, and the savvy creators will incorporate videos of their process as a form of authenticity marker to their audience. Even the most unscrupulous 'prompt artist' cannot do that. And they have certainly tried*". Art critics also have a say here: some of them compare artworks generated by AI systems to those produced by monkeys for both lack "intentionalism" (Fadeeva, 2023), others – consider a mixture of digital technologies and traditional art a new reality (Stepanov, 2022; Bylieva & Krasnoschekov, 2023) and some claim that the use of such technologies is nothing but another step towards dehumanization and demonstrate that an ordinary person not always understands which artwork is human-made and which is generated by AI (Panteleev, 2023).

2.2. Plagiarism, violation of copyrights and other risks

Another two claims that we need to discuss is whether generative AI can cause unfair competition and whether or not the industry actually considers that producers and owners of generative AI systems violate copyrights[37].

"Yes, on both counts. As the numerous lawsuits and litigations filed earlier this year attest to, the developers of these platforms have to a greater or lesser extent, known about the existence of vast numbers of copyrighted material in their AI datasets. This is the big elephant in the room so to speak. Without exaggeration, the use of copyrighted material on this scale is so large and unprecedented it is almost an abstract entity, which makes it in some cases difficult to prove. But the proof is certainly out there.

The other side of the equation too is compensation. Creatives are being replaced, as simple as that. There are too many numerous examples to count, but there is a substantial material impact on the creative industries, which has traditionally been underpaid and relies largely on a patronage model. I always thought creatives were the canaries in the coal mine, so to speak. If left unchecked and unregulated, then there will not be many industries which would not be materially affected in some way by AI.

A couple of things to note here: one is this populist notion that creative people are Luddites who are against technology. I don't believe that rhetoric for a moment. It is not the technology that is the issue, it is the abuse of it as I noted earlier. Automation in factory work is arguably necessary as repetitive tasks in particular environments pose a risk to life. The same cannot be said for automating the culture we collectively view as sacred, and like any medium, can be turned to nefarious ends. So therefore, it's not just a question of copyright, but also of the impact of how the technology affects us in our day to day lives".

All of the above can be supported by the demands of SAG-AFTRA[38] and WGA[39] strikes and those of the Authors Guild[40] as well as by lawsuits against producers of generative AI systems such as: 1) Sarah Andersen's, Kelly McKernan's and Karla Ortiz' class action versus STABILITY AI LTD, Delaware corporation and DEVIANTART[41]; 2) Authors Guild v. OpenAI Inc., where the most notorious claim is that OpenAI doesn't even deny that they train their systems of materials protected by copyright[42].

The opinion expressed by the English-speaking respondents correlates with it too: 72.5 % of the English-speaking responders agree that producers of generative AI systems violate copyrights, whereas 11.1 % of them disagree with this notion (Fig. 7). Even more – 76.9 %

37 Case updates. Stable Diffusion litigation. (2023, October 31). https://clck.ru/36n4fM

38 We're Fighting for the Survival of Our Profession. SAG-AFTRA Strike. https://clck.ru/36n39G

39 WGA Contract 2023. Summary of the 2023 WGA MBA. https://clck.ru/35shcD

40 Artificial Intelligence. The Authors Guild. https://clck.ru/36n4h8

41 United States District Court Northern District of California San Francisco Division. Stable Diffusion litigation. https://clck.ru/36n4hr

42 Authors Guild v. OpenAI Inc. (1:23-cv-08292). Court Listener. https://clck.ru/36n4mC

of the responders believe that such companies violate intellectual property rights, however, 14.5 % express the opposite opinion (Fig. 8).

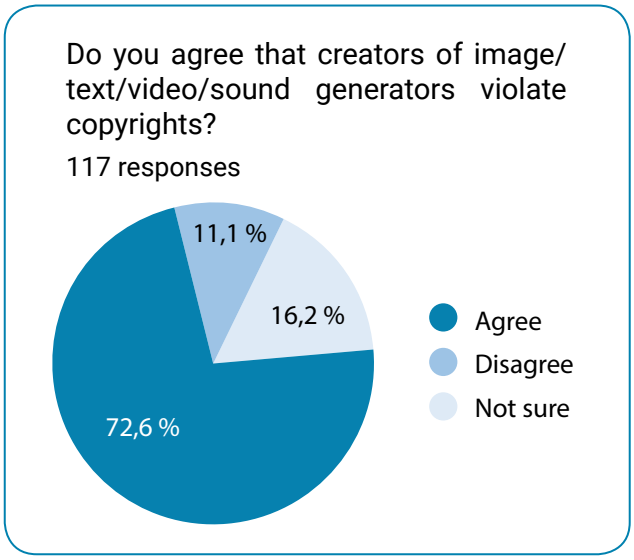


Fig. 7

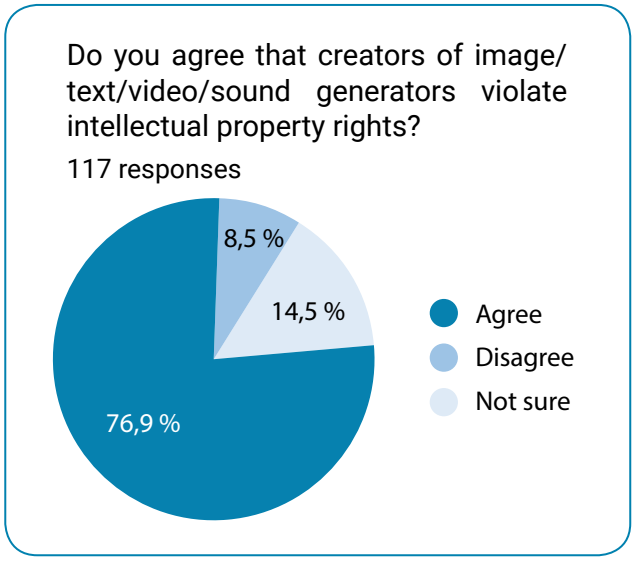


Fig. 8

The Russian-speaking audience demonstrated the opposite trend – 50 % of it don't think that producers of generative AI systems violate copyrights (Fig. 9) and 58.3 % disagree on the notion that such companies violate intellectual property rights (Fig. 10). Only 19.4 % of the Russian-speaking responders share their foreign colleagues' point of view on violation of copyrights by producers of generative AI systems (Fig. 9) and only 16.7 % support the opinion about violation of intellectual property rights by such companies (Fig. 10). In both cases, a big percentage of responders are not sure about their positions – it's 30.6 % (Fig. 9) and 25 % (Fig. 10) respectively.

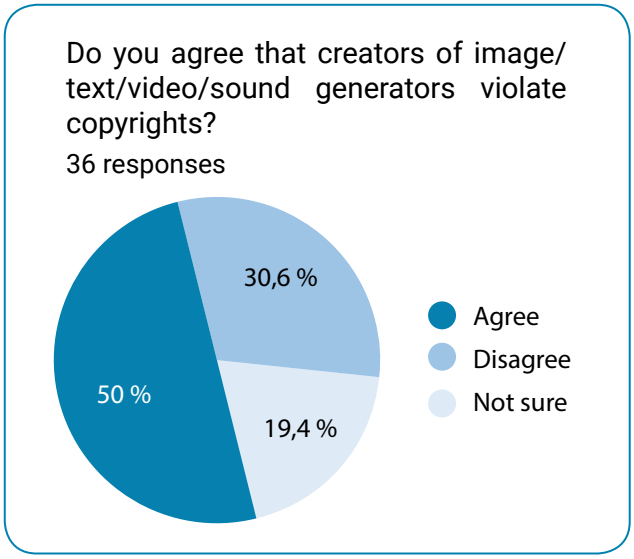


Fig. 9

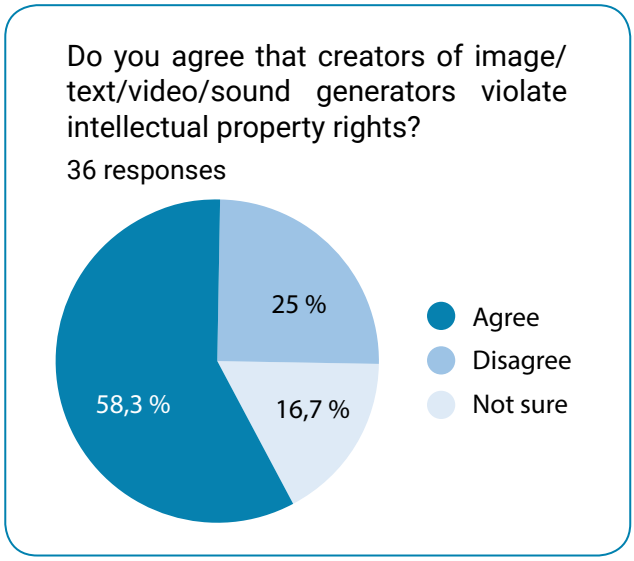


Fig. 10

The SAG-AFTRA strike made it perfectly clear: they consider AI an existential threat to their profession, thus the slogan "We're fighting for the survival of our profession" and what they mean is generative AI systems allow studios to hire an actor for one working day, pay them a minimum wage but then reproduce the image and the voice of this actor whenever and however they want[43]. Hence, another question – will the creative industry survive the impact of such a mass-usage of generative AI systems? Or it is a real threat that should not be ignored before it is too late?

"*In my line of work, I've seen other practitioners charge good money to effectively run photographs through AI filters and call it the finished result. In order to adapt, I've leaned into the process and the contextualisation of the work as the primary generators of value, because it is an authentic representation of human endeavour.*

The threat has already been and gone, and my niche industry trained. However, as the adage goes: you get what you pay for. There will always be a demand for human led curation, restoration and contextualisation in my particular field, and it has led to some interesting developments on how to make revenue by drawing on your strengths, rather than compensate for weaknesses. Generative AI simply cannot replicate many of the processes we've set up. We'll quietly do our own thing, and leave it at that" – comments Mr. Lloyd.

The opinions shared by the English-speaking responders are a bit less optimistic – 60.7 % suggest that generative AI poses a real threat to the creative industry's jobs, 18.8 % disagree with them, 17.9 % aren't sure and 2.6 % claim that they have already been replaced with generative AI (Fig. 11).

Again, the Russian-speaking audience showed the directly opposite trend: 75 % of the responders don't see generative AI as a threat to the industry, 16.7 % do, 8.3 % aren't sure and none of the responders have been replace with generative AI yet (Fig. 12).

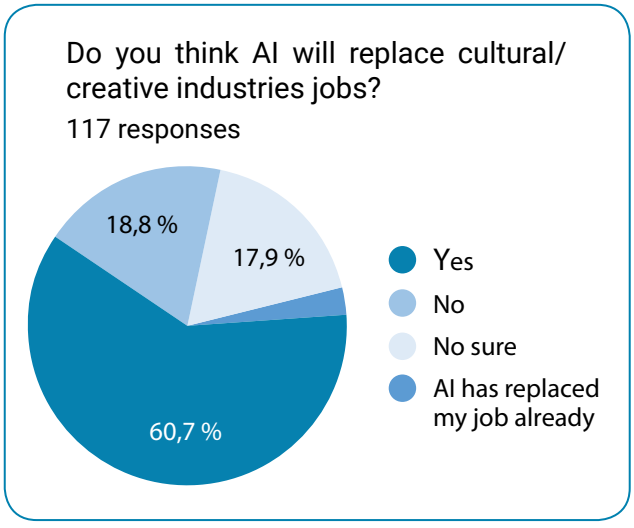


Fig. 11

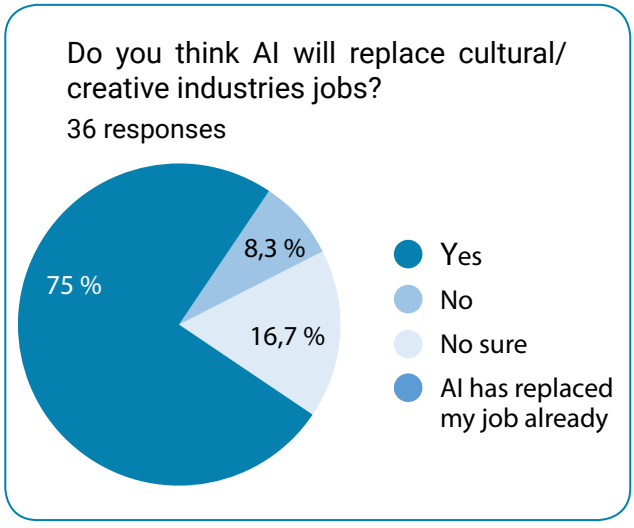


Fig. 12

[43] We're Fighting for the Survival of Our Profession. SAG-AFTRA Strike. https://clck.ru/36n39G

It is worth-mentioning that the responses of the Russian-speaking audience correlate with the general view of the Russian creative industry on these technologies – they tend to see it only as an instrument and make philosophical commentary that instruments do not have a soul and therefore, cannot be a creator – meaning, they will never be able to replace human creators[44]. But does it mean there can be benefits of using generative AI as an instrument in the creative industry? "*First and foremost, it's important to make some distinctions which are being conflated in the discussions about AI today. Fundamentally as an aid or tool in specific applications, AI processes make things possible which were not possible before, and they are specific to particular workflows. In my career working with archive visual material – such as photographic scans – upscaling to a larger resolution is only possible with the use of AI. There are other workflows which are highly specialised where the application of AI as a tool or aid is simply part of much longer technical process.*

The problem arises when users conflate the idea of an 'aid' or 'tool' with the wholesale creation of a new piece of material; whether or not it's a piece of artwork in the style of a living artist, or a piece of prose generated from a few text prompts. This 'generative' usage of an AI process is different to the usage I described above. It is not an aid for example to create a Derivative or Transformative Work in my opinion, merely an imitation of something created by someone else.

*To put it another way: there's a spectrum between *use* and *abuse*. I've had many discussions with creatives about the use of Generative AI. I know one artist who uses Midjourney to simply generate some different compositions around a subject, and then picks one to then as a visual reference for an entirely original work done by hand. I can imagine that would be a timesaver when faced with commercial deadlines, and to me, an acceptable use of the technology.*

Let's compare that with an instance I can think of where a self-published author won a prize based on their cover art, only to discover the artist had charged a considerable sum of money to create a cover featuring entirely Generated art collaged together. It is arguable whether or not the generated art could really be considered a Derivative or Transformative Work as something like that under UK law requires 'itself [to] be an original work of skill, labour and judgement'. Further, 'minor alterations that do not substantially alter the original would not qualify.'

In the case of the book cover artist, it could be argued the only creative act involved was the final arrangement of composition of the generated assets. In the case of my artist acquaintance, the process of creation was entirely by human hand and imagination.

From a generative standpoint: the only possible way I can think of for it to be truly ethical is if the dataset was only based on original works that you have provided, or taken from the Public Domain. Sadly, as we all know that is not the case".

[44] At Gorkiy fest, the problem of neural networks participation in cinematography was discussed. Bulleten Kinoprokatchika. https://clck.ru/36n4pf

Again, all of mentioned points can be supported by the results of the investigations conducted by the House of Commons earlier this year – the experts participated in them expressed the concern of the abuse of generative AI technologies that becomes possible due to the identified legal gaps and include the rise of plagiarism, replacement human creators with generative AI and violation of other rights, however, they also suggested to encourage the use of AI technologies (not just the generative ones) in the industry because of their enormous potential, but only when such technologies are going to be used ethically[45] [46].

As another case of abuse of the generative AI technologies, we can provide an example of the most recent and quite scandalous Russian lawsuit – Alena Andronova against the Tinkoff bank. A dubbing actress, she recorded her voice for the bank needs but then it got synthesized and used by a third party to dub several types of illegal content that, allegedly, resulted in her losing contracts[47].

And what are other risks the industry has been facing due to the mass-usage of generative AI technologies? "As noted, unscrupulous actors simply wanting to cash in on an industry which is small but perpetually of great interest to the public. Many historians rightfully are alarmed at the decontextualisation of historical material and the lack of attribution. I agree with them in this respect. I'm not entirely sure what the way out is, but I'm confident the industry is small enough to not go into cataclysmic collapse because of the introduction of AI. Practitioners should be aware of their ethical responsibilities in the pursuit of their work".

2.3. Labeling products of generative AI

From the analysis of the Chinese approach towards the legal regulation of generative AI, we conclude that AI-labeling is seen as a measure to protect both artists and users of generative AI systems[48]. Recently, several companies have begun offer their services to do the exactly the same[49, 50] – to create "AI nutrition labels" in order to increase transparency and encourage responsible usage of generative AI systems, so according to their claims, such a simple action as putting a label of "AI ingredients" can prevent the abuse of these technologies.

---

45 Connected tech: AI and creative technology: Eleventh Report of Session 2022–23. (2023). UK Parliament. https://clck.ru/36n3Sf

46 The governance of artificial intelligence: interim report. Ninth Report of Session 2022–23. (2023). UK Parliament. https://clck.ru/36n3TN

47 Information on the primary document № M-6609/2023. Oficialniy Portal Sudov Moskvy. https://clck.ru/36KzHu

48 生成式人工智能服务管理暂行办法. 1994. No. 143. 国家互联网信息办公室. (2023). 第15号. https://goo.su/fbbG

49 AI Nutrition Facts. Twilio. https://clck.ru/36n4xc

50 Open Ethics Label: AI nutrition labels. Open Ethics. https://clck.ru/36n4yq

From monitoring the news, we also can suggest that politicians[51] and digital-security experts[52] support these claims, furthermore, all of them suggest that such labeling must be obligatory because otherwise we cannot prevent the on-going spread of misinformation and "deep-fakes", which is also crucial, considering the fact that the British government has already linked it to such a dangerous threat as terrorism[53].

But does the industry agree that this measure can be as effective as the providers[54, 55] of AI-labeling services claim? "*I very much doubt it, though it would be a welcome legal requirement. I akin to any form of advertising as noted earlier. Consumers should be aware if something they see or read is generated by AI, and held to the same regulatory standards as advertisers with their products. 'False Advertising' is a well-established regulatory process. Time and time again when a form of marketing by organisations has been called out for using AI generated assets, the initial denials are usually met with a begrudging acceptance followed by a proclamation to adjust their working practices*".

Our responders almost unanimously they said "Yes, products of generative AI should be labeled us such" - 88% of the English speakers support this idea and only 7.7% find it unnecessary (Fig. 13), and 80.6% of the Russian speaker consider that labeling AI-products should be obligatory, whereas only 13.9% dislike this idea (Fig. 14).

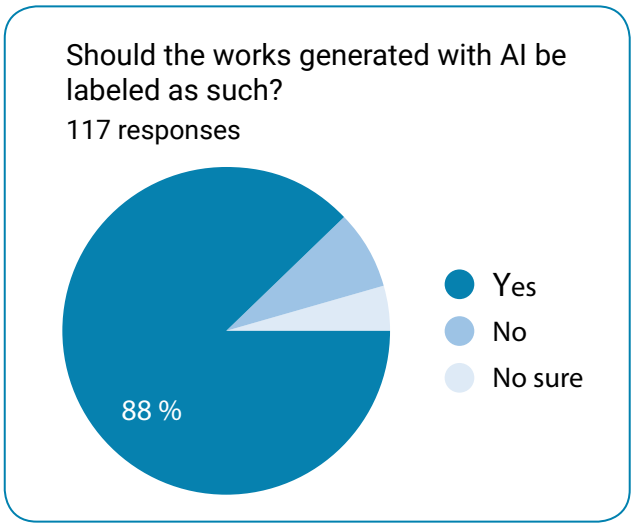


Fig. 13

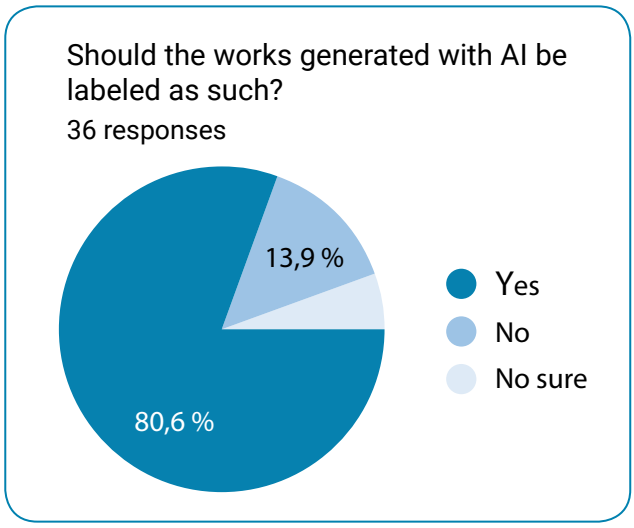


Fig. 14

51 AI generated content should be labelled, EU Commissioner Jourova says. Reuters. https://clck.ru/36n5B8

52 Ministry of Digital Development was offered to introduce marking of the content created with neural networks. (2023, May 15). TASS. https://clck.ru/34RfkG

53 AI safety summit. Department For Science, Innovation and Technology. https://clck.ru/36n3zq

54 AI Nutrition Facts. Twilio.https://clck.ru/36n4xc

55 Open Ethics Label: AI nutrition labels. Open Ethics. https://clck.ru/36n4yq

It is necessary to add that technologically, it is possible to effectively label or, as other researchers call it "to watermark" all sorts of data, including digital audio (Patil & Shelke, 2023) and even do it invisibly if needed (Liu et al., 2022). Furthermore, it is possible to create a screen-shooting resistible watermark (Cao et al., 2023). Various watermarking methods can help with content authentication (Yuan et al., 2024), protection and even recovery of it (M. Swain & D. Swain, 2022). However, other research works demonstrate that a watermark within neural networks, for example, should not be seen as a panacea because it can be removed (Aiken et al., 2021).

2.4. The voice of the industry being heard

"*Intellectual Property constitutes a major contributor to the national economy of the United Kingdom; from our scientific research to our cultural output in the arts. As with many countries, arts funding and access has always been challenging, and the advent of Generative AI will certainly accelerate some negative aspects of it. I believe it is in the interests of our legal framework to regulate as quickly as possible*".

One of the questions of our survey was about whether our responders believed that the current laws of their country could protect them as professionals against the negative impact of the generative AI, and the gathered data supports the opinion about the inability of states adequately and timely eliminate concerns of their nationals being a cause of public political distrust in government – 72.6 % of the English-speaking responders do not trust the current legislature of their countries with it, 3.4 % think that they can be protected by the existing legal norms, 13.7 % are not sure and 10.3 % are consumers of the creative industry products, so this question wasn't meant for them (Fig. 15).

The Russian-speaking audience is again, demonstrates a more optimistic attitude, nevertheless, 50 % of the responders don't trust the current laws of their countries with the protection against generative AI, 16.7 % believe that they are already protected enough and 33.3 % are not sure (Fig. 16).

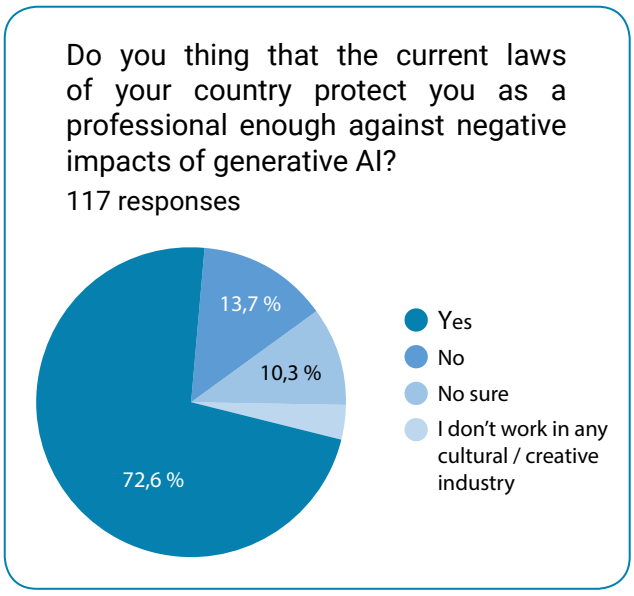


Fig. 15

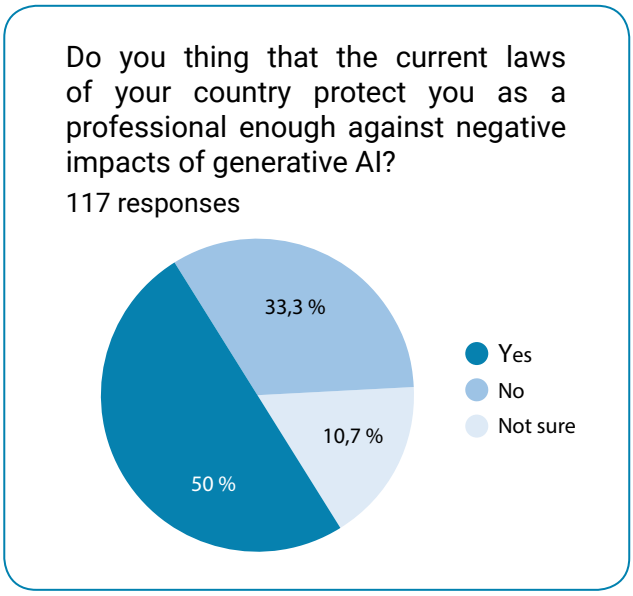


Fig. 16

But the voice of the industry clearly hasn't been ignored – numerous law projects have been appearing all over the globe the final goal of which is to protect both the creative industry and consumers of its products, and to increase transparency and responsibility of the usage of generative AI systems.

The WGA, for example, ended their strike in September – the agreement has been reached and to be ratified, so according to it: 1) AI can't write or rewrite literary material, and AI-generated material will not be considered source material under the MBA, meaning that AI-generated material can't be used to undermine a writer's credit or separated rights; 2) A writer can choose to use AI when performing writing services, if the company consents and provided that the writer follows applicable company policies, but the company can't require the writer to use AI software (e.g., ChatGPT) when performing writing services; 3) The Company must disclose to the writer if any materials given to the writer have been generated by AI or incorporate AI-generated material, 4) The WGA reserves the right to assert that exploitation of writers' material to train AI is prohibited by MBA or other law[56].

The voice of Alena Andronova also has been heard – even though the court left her case without movement[57], after she teamed-up with the Union of Narrators and other victims whose voices "have been stolen"[58] to prove that a human voice is a biometric data and thus, shouldn't be collected without consent, the Soviet of Federation has come up with a decision to protect human voices from the negative impact of generative AI and deep-synthesis technologies and to prevent further legal collisions[59].

The Senate of the USA has been listening to the voice of the industry too – they've come up with a similar to the Russian legal act that is currently known as "No fakes law" and that is supposed to put under the legal protection "image, voice and visual likeness" of individuals for the entire life period for 70 years after the death on an individual[60].

The European Parliament, apparently, have found inspiration in the Chinese approach[61] towards regulations of generative AI because now they demand from producers of digital AI systems the following: 1) Disclosing that the content was generated by AI; 2)

56 WGA contract 2023. Summary of the 2023 WGA MBA. https://clck.ru/35shcD

57 Information on the primary document № M-6609/2023. Oficialniy Portal Sudov Moskvy. https://clck.ru/36KzHu

58 Andronova, A. (2023, August 30). We beg to protect our voices from theft and fraud!. CHANGE ORG. https://clck.ru/36KzMK

59 Federation Council was offered to protect a human voice and its synthesis. PRAVO.RU. https://clck.ru/36j2Sy

60 Senate Legislative Counsel Draft Copy of EHF23968 GFW – To protect the image, voice, and visual likeness of individuals, and for other purposes. Senate GOV. https://clck.ru/36nutL

61 生成式人工智能服务管理暂行办法. 1994. No. 143. 国家互联网信息办公室. (2023). 第15号. https://goo.su/fbbG

Designing the model to prevent it from generating illegal content; 3) Publishing summaries of copyrighted data used for training[62].

Additionally, corporations like Microsoft[63], Adobe[64] and Google[65] have decided to implement protection for users of their generative AI systems against copyright and IP-related lawsuits, even promising to pay legal damages in such cases. Microsoft explains that the new measures will also help human creators "retain control of their rights under copyright law and earn a healthy return on their creations"[66].

Conclusions

The conducted research revealed that currently there is no universal understanding of whether generative AI can be considered a subject of copyright law and its products – objects of copyright law/IP rights as well as there is no international legal framework that could be able to regulate the mass-use of such technologies. Should such regulations not be developed promptly, the harm to the creative industry and through it – to state economics will be inevitable. Among the risks that the unregulated use of generative AI systems our analysis identified the following: 1) violation of copyright and IP rights; 2) violation of moral rights; 3) violation of labor rights; 4) disruption of labor market; 5) violation of customers rights; 6) mass-production of illegal content; 7) the crisis of originality; 8) unfair competition; 9) public distrust in government; 10) public disorder; 11) extremism and terrorism.

To minimize the identified risks, it is important to promptly develop new international and national legal frameworks, which will help increase accountability of producers, owners and users of generative AI systems and will make them liable for abuse of these technologies: "*First and foremost, the developers of these AI services should be open to scrutiny and not rely on technical obfuscation and held accountable for their training data. No one would be having a problem with this if the developers simply stuck to Public Domain material and Opt-in participation. Second, a fairer form of compensation for creators whose work has ended up in these training sets. If we have the means to scrape data en masse, then we have the means to fairly acknowledge the role of creatives in this process and pay them accordingly. Third, commercial usage should be formalised and regulated. The stock photography industry is very much thriving and well established with comparatively little abuse of the system which makes commercial*

62 EU AI Act: first regulation on artificial intelligence. EU Parlaiment. https://clck.ru/36n5Lv

63 Microsoft announces new Copilot Copyright Commitment for customers. Microsoft. https://clck.ru/36n5MQ

64 Adobe offers copyright indemnification for Firefly AI-based image app users. Computer World. https://clck.ru/36n5Mx

65 Shared fate: Protecting customers with generative AI indemnification. Google. https://clck.ru/36n5NP

66 Microsoft announces new Copilot Copyright Commitment for customers. Microsoft. https://clck.ru/36n5MQ

sense for the platform holders and the creatives who submit their work to them. I can't see why an opt-in arrangement regarding Generative AI can't be implemented in some form to stop the rampant abuse. Forth, search engines in particular should be vigilant in how they present AI generated material. How this is achieved on a technical level is not for me to say, but again, possible".

We can also state that countries with different regimes have begun to adopt more less similar measures close to those enforced in China[67], which include: 1) transparency about the data used for training; 2) generative AI-products labeling; 3) liability for violation of copyright and intellectual property rights; 4) protection of the image, voice and likeness of an individual. In our opinion, in the foreseeable future the use of generative AI systems will be regulated by similar measures on the international level as well.

In conclusion, we would like to highlight that the question of ethical use of generative AI goes far beyond the question "Who's the author?" and affects not only the creative industry but has an impact on states economies and even democratic institutions themselves as shown by our analysis, hence the necessity of filling in the existing legal gaps, including such a simple, at first glance, thing as the lack of appropriate terminology.

References

Agibalova, E. N., & Perekrestova, E. A. (2020). Copyright for the works created by artificial intelligence. *Ehpokha nauki*, *24*, 124–126. (In Russ.). https://doi.org/10.24411/2409-3203-2020-12424

Aiken, W., Kim, H., Woo, S. S., & Ryoo, J. (2021). Neural network laundering: Removing black-box backdoor watermarks from deep neural networks. *Computers & Security*, *106*, 102277. https://doi.org/10.1016/j.cose.2021.102277

Bylieva, D., & Krasnoschekov, V. (2023). The original and a copy: a technological challenge to art. *Bulletin of the Moscow Region State University*. Series: Philosophy, 2, 77–91. (In Russ.). https://doi.org/10.18384/2310-7227-2023-2-77-91

Cao, F., Wang, T., Guo, D., Li, J., & Qin, C. (2023). Screen-shooting resistant image watermarking based on lightweight neural network in frequency domain. *Journal of Visual Communication and Image Representation*, *94*, 103837. https://doi.org/10.1016/j.jvcir.2023.103837

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., De Prado, M. L., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, 101896. https://doi.org/10.1016/j.inffus.2023.101896

Fadeeva, T. E. (2023). "Union" of an artist with a non-human agent: utopia or a working model of artistic production? Izvestiya of the Samara Science Centre of the Russian Academy of Sciences. *Social, Humanitarian, Biomedical Sciences*, *25*(88), 108–115. (In Russ.). https://doi.org/10.37313/2413-9645-2023-25-88-108-115

Fenwick, M., & Jurčys, P. (2023). Originality and the future of copyright in an age of generative AI. *Computer Law & Security Review*, 105892. https://doi.org/10.1016/j.clsr.2023.105892

Küçükkömürler, S., & Özkan, T. (2022). Political interest across cultures: The role of uncertainty avoidance and trust. *International Journal of Intercultural Relations*, *91*, 88–96. https://doi.org/10.1016/j.ijintrel.2022.09.004

Liu, G., Xiang, R., Liu, J., Pan, R., & Zhang, Z. (2022). An invisible and robust watermarking scheme using convolutional neural networks. *Expert Systems With Applications*, *210*, 118529. https://doi.org/10.1016/j.

[67] 生成式人工智能服务管理暂行办法. 1994. No. 143. 国家互联网信息办公室. (2023). 第15号. https://goo.su/fbbG

eswa.2022.118529

Panteleev, A. F. (2023). The problem of comparative evaluation of paintings created by an artist and generated by a neural network. Izvestiya of Saratov University. *Philosophy. Psychology. Pedagogy*, *23*(3), 326–330. (In Russ.). https://doi.org/10.18500/1819-7671-2023-23-3-326-330

Patil, A. P., & Shelke, R. (2023). An effective digital audio watermarking using a deep convolutional neural network with a search location optimization algorithm for improvement in Robustness and Impercepetibility. *High-Confidence Computing*, 100153. https://doi.org/10.1016/j.hcc.2023.100153

Somenkov, S. A. (2019). Artificial intelligence: from object to subject? *Courier of the Kutafin Moscow State Law University*, *2*(54), 75–85. (In Russ.). https://doi.org/10.17803/2311-5998.2019.54.2.075-085

Sparkes, M. (2022). AI copyright. *New Scientist*, *256*(3407), 17. https://doi.org/10.1016/s0262-4079(22)01807-3

Stepanov, M. A. (2022). De-Autonomy of Post-Human Imagination: New Directions in the Theory of Art. *Actual Problems of Theory and History of Art* (No.*12*, pp. 663–673). (In Russ.). http://dx.doi.org/10.18688/aa2212-07-53

Stokel-Walker, C. (2023). ChatGPT's knowledge of copyrighted novels highlights legal uncertainty of AI. *New Scientist*, *258*(3438), 13. https://doi.org/10.1016/s0262-4079(23)00837-0

Stroppe, A. (2023). Left behind in a public services wasteland? On the accessibility of public services and political trust. *Political Geography*, *105*, 102905. https://doi.org/10.1016/j.polgeo.2023.102905

Swain, M., & Swain, D. (2022). An effective watermarking technique using BTC and SVD for image authentication and quality recovery. *Integration*, *83*, 12–23. https://doi.org/10.1016/j.vlsi.2021.11.004

Torres, G. & Bellinger, N. (2014). The Public Trust: The Law's DNA. *Cornell Law Faculty Publications*. Paper 1213. http://scholarship.law.cornell.edu/facpub/1213

Wan, Y., & Lu, H. (2021). Copyright protection for AI-generated outputs: The experience from China. *Computer Law & Security Review*, *42*, 105581. https://doi.org/10.1016/j.clsr.2021.105581

Yuan, Z., Zhang, X., Wang, Z., & Yin, Z. (2024). Semi-fragile neural network watermarking for content authentication and tampering localization. *Expert Systems With Applications*, *236*, 121315. https://doi.org/10.1016/j.eswa.2023.121315

Authors information

Natalia I. Shumakova – Associate Professor, Department of Constitutional and Administrative Law, Law Institute, South Ural State University (National Research University), Chelyabinsk, Russia
Address: 76 Lenin Str., 454080 Chelyabinsk, Russian Federation
E-mail: shumakovani@susu.ru
ORCID ID: http://orcid.org/0009-0004-6053-0650
RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=1211522

Jordan J. Lloyd – Creative Director, Unseen History
Address: Howes Farm, Doddinghurst Road, Brentwood, Essex, CM15 0SG, United Kingdom
E-mail: jordan@unseenhistories.com
ORCID ID: https://orcid.org/0009-0007-8733-7261

Elena V. Titova – Dr. Sci. (Law), Associate Professor, Department of Constitutional and Administrative Law, Law Institute, South Ural State University (National Research University)
Address: 76 Lenin Str., 454080 Chelyabinsk, Russian Federation
E-mail: titovaev@susu.ru
ORCID ID: http://orcid.org/0000-0001-9453-3550
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57201640405
Google Scholar ID: https://scholar.google.ru/citations?user=Pqj6OiQAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=451302

Authors' contributions

The idea of the article is joint and belongs to Natalia I. Shumakova and Jordan J. Lloyd.
Natalia I. Shumakova formulated the idea; drafted the manuscript; developed the methodology; organized sociological surveys; collected and analyzed literature and legislation; formulated key conclusions, proposals and recommendations.
Jordan J. Lloyd drafted, processed and presented his expert opinion on the key provisions of the article; sampled media publications; interpreted the overall results of the study.
Elena V. Titova analyzed legislation; considered the processes occurring in the creative industry from the viewpoint of public/political distrust manifestation; partially collected and analyzed scientific literature.

Conflict of interest

The authors declare no conflict of interest.

Financial disclosure

The research had no sponsorship.

Acknowledgements

The authors are grateful to the Editorial Office of the Journal of Digital Technologies and Law for their assistance in conducting a sociological survey in the Journal's Telegram channel at https://t.me/JournalDTL

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – October 31, 2023
Date of approval – November 20, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:34.096:347.211:004.8
EDN: https://elibrary.ru/wxwsvu
DOI: https://doi.org/10.21202/jdtl.2023.38

На пути к правовому регулированию генеративного ИИ в творческой индустрии

Наталья Игоревна Шумакова ✉

Южно-Уральский государственный университет (национальный исследовательский университет)
г. Челябинск, Российская Федерация

Джордан Дж. Ллойд

Компания «Unseen History»
г. Эссекс, Великобритания

Елена Викторовна Титова

Южно-Уральский государственный университет (национальный исследовательский университет)
г. Челябинск, Российская Федерация

Ключевые слова

авторское право, генеративный искусственный интеллект, интеллектуальная собственность, искусственный интеллект, международное право, нейронная сеть, объект авторского права, субъект авторского права, творческая индустрия, цифровые технологии

Аннотация

Цель данной статьи – ответить на следующие вопросы: 1. Может ли генеративный искусственный интеллект быть субъектом авторского права? 2. К каким рискам может привести нерегулируемое использование систем генеративного искусственного интеллекта? 3. Какие правовые пробелы необходимо закрыть для минимизации таких рисков?

Методы: сравнительно-правовой анализ, социологический метод, частно-социологический метод, количественный и качественный анализ данных, статистический анализ, метод кейсов, индукция, дедукция.

Результаты: авторы выявили ряд рисков, возникающих при нерегулируемом использовании генеративного искусственного интеллекта в творческой индустрии, среди которых нарушение авторского и трудового права, нарушение прав потребителей и рост недоверия населения к власти. Авторы полагают, что оперативная разработка новых правовых норм может минимизировать эти риски. В заключение констатируется, что государства уже начали осознавать опасность игнорирования негативного влияния генеративного искусственного интеллекта на творческую индустрию, что обусловливает разработку аналогичных правовых норм в государствах с совершенно разными режимами.

✉ Контактное лицо

Научная новизна: в работе проведено комплексное исследование влияния генеративного искусственного интеллекта на творческую индустрию с двух точек зрения: с позиции права и с позиции индустрии. Эмпирическую базу составляют два международных исследования и экспертное мнение представителя отрасли. Такой подход позволил авторам повысить объективность исследования и получить результаты, которые могут быть использованы для поиска практического решения выявленных рисков. Проблема непрерывного развития и роста популярности систем генеративного искусственного интеллекта выходит за рамки вопроса «кто автор?», поэтому ее необходимо решать путем внедрения иных, нежели уже существующих, механизмов и правил. Данная точка зрения подтверждается не только результатами проведенных исследований, но и анализом текущих судебных исков к разработчикам систем генеративного искусственного интеллекта.

Практическая значимость: полученные результаты могут быть использованы для ускорения разработки универсальных правовых норм, правил, инструментов и стандартов, отсутствие которых в настоящее время представляет угрозу не только для прав человека, но и для ряда отраслей творческой индустрии и других областей.

Для цитирования

Шумакова, Н. И., Ллойд, Дж. Дж., Титова, Е. В. (2023). На пути к правовому регулированию генеративного ИИ в творческой индустрии. *Journal of Digital Technologies and Law*, *1*(4), 880–908. https://doi.org/10.21202/jdtl.2023.38

Список литературы

Агибалова, Е. Н., Перекрёстова, Е. А. (2020). Право авторства на произведения, созданные искусственным интеллектом. *Эпоха науки*, *24*, 124–126. https://doi.org/10.24411/2409-3203-2020-12424

Быльева, Д. С., Краснощеков, В. В. (2023). Оригинал и копия: технологический вызов искусству. *Вестник Московского государственного областного университета. Серия: Философские науки*, 2, 77–91. https://doi.org/10.18384/2310-7227-2023-2-77-91

Пантелеев, А. Ф. (2023). Проблема сравнительной оценки картин, созданных художником и сгенерированных нейросетью. *Известия Саратовского университета. Новая серия. Серия: Философия. Психология. Педагогика*, *23*(3), 326–330. https://doi.org/10.18500/1819-7671-2023-23-3-326-330

Соменков, С. А. (2019). Искусственный интеллект: от объекта к субъекту? *Вестник Университета имени О. Е. Кутафина*, *2*(54), 75–85. https://doi.org/10.17803/2311-5998.2019.54.2.075-085

Степанов, М. А. (2022). Деавтономия постчеловеческого воображения: новые направления в теории искусства. В сб: *Актуальные проблемы теории и истории искусства* (№ 12, с. 663–673). http://dx.doi.org/10.18688/aa2212-07-53

Фадеева, Т. Е. (2023). «Союз» художника с нечеловеческим агентом – утопия или рабочая модель художественного производства? *Известия Самарского научного центра Российской академии наук. Социальные, гуманитарные, медико-биологические науки*, *25*, 1(88), 108–115. https://doi.org/10.37313/2413-9645-2023-25-88-108-115

Aiken, W., Kim, H., Woo, S. S., & Ryoo, J. (2021). Neural network laundering: Removing black-box backdoor watermarks from deep neural networks. *Computers & Security*, *106*, 102277. https://doi.org/10.1016/j.cose.2021.102277

Cao, F., Wang, T., Guo, D., Li, J., & Qin, C. (2023). Screen-shooting resistant image watermarking based on lightweight neural network in frequency domain. *Journal of Visual Communication and Image Representation*, *94*, 103837. https://doi.org/10.1016/j.jvcir.2023.103837

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., De Prado, M. L., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, 101896. https://doi.org/10.1016/j.inffus.2023.101896

Fenwick, M., & Jurčys, P. (2023). Originality and the future of copyright in an age of generative AI. *Computer Law & Security Review*, 105892. https://doi.org/10.1016/j.clsr.2023.105892

Küçükkömürler, S., & Özkan, T. (2022). Political interest across cultures: The role of uncertainty avoidance and trust. *International Journal of Intercultural Relations*, *91*, 88–96. https://doi.org/10.1016/j.ijintrel.2022.09.004

Liu, G., Xiang, R., Liu, J., Pan, R., & Zhang, Z. (2022). An invisible and robust watermarking scheme using convolutional neural networks. *Expert Systems With Applications*, *210*, 118529. https://doi.org/10.1016/j.eswa.2022.118529

Patil, A. P., & Shelke, R. (2023). An effective digital audio watermarking using a deep convolutional neural network with a search location optimization algorithm for improvement in Robustness and Impercepetibility. *High-Confidence Computing*, 100153. https://doi.org/10.1016/j.hcc.2023.100153

Sparkes, M. (2022). AI copyright. *New Scientist*, *256*(3407), 17. https://doi.org/10.1016/s0262-4079(22)01807-3

Stokel-Walker, C. (2023). ChatGPT's knowledge of copyrighted novels highlights legal uncertainty of AI. *New Scientist*, *258*(3438), 13. https://doi.org/10.1016/s0262-4079(23)00837-0

Stroppe, A. (2023). Left behind in a public services wasteland? On the accessibility of public services and political trust. *Political Geography*, *105*, 102905. https://doi.org/10.1016/j.polgeo.2023.102905

Swain, M., & Swain, D. (2022). An effective watermarking technique using BTC and SVD for image authentication and quality recovery. *Integration*, *83*, 12–23. https://doi.org/10.1016/j.vlsi.2021.11.004

Torres, G. & Bellinger, N. (2014). The Public Trust: The Law's DNA. *Cornell Law Faculty Publications*. Paper 1213. http://scholarship.law.cornell.edu/facpub/1213

Wan, Y., & Lu, H. (2021). Copyright protection for AI-generated outputs: The experience from China. *Computer Law & Security Review*, *42*, 105581. https://doi.org/10.1016/j.clsr.2021.105581

Yuan, Z., Zhang, X., Wang, Z., & Yin, Z. (2024). Semi-fragile neural network watermarking for content authentication and tampering localization. *Expert Systems With Applications*, *236*, 121315. https://doi.org/10.1016/j.eswa.2023.121315

Информация об авторах

Шумакова Наталья Игоревна – доцент кафедры конституционного и административного права, Южно-Уральский государственный университет (национальный исследовательский университет)
Адрес: 454080, Российская Федерация, г. Челябинск, пр. Ленина, 76
E-mail: shumakovani@susu.ru
ORCID ID: http://orcid.org/0009-0004-6053-0650
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=1211522

Ллойд Джордан Дж. – Шеффилдский университет; креативный директор, компания «Unseen History»
Адрес: Хоуес Фарм, Доддингхерст Роуд, Брентвуд, Эссекс, CM15 0SG, Великобритания
E-mail: jordan@unseenhistories.com
ORCID ID: https://orcid.org/0009-0007-8733-7261

Титова Елена Викторовна – доктор юридических наук, доцент, директор Юридического института, заведующий кафедрой конституционного и административного права, Южно-Уральский государственный университет (национальный исследовательский университет)
Адрес: 454080, Российская Федерация, г. Челябинск, пр. Ленина, 76
E-mail: titovaev@susu.ru
ORCID ID: http://orcid.org/0000-0001-9453-3550
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57201640405
Google Scholar ID: https://scholar.google.ru/citations?user=Pqj6OiQAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=451302

Вклад авторов

Идея статьи является совместной и принадлежит Н. И. Шумаковой и Дж. Дж. Ллойду.
Н. И. Шумакова осуществляла формулирование идеи; выполняла составление черновика и чистовика рукописи; разработала дизайн методологии; организовала проведение социологических опросов; осуществляла сбор и анализ литературы и законодательства; сформулировала ключевые выводы, предложения и рекомендации.
Дж. Дж. Ллойд составил, обработал и предоставил свое экспертное мнение по ключевым положениям статьи; провел выборку публикаций в медиа; осуществлял интерпретацию общих результатов исследования.
Е. В. Титова осуществляла анализ законодательства; рассмотрела с точки зрения проявления публичного/политического недоверия процессы, происходящие в творческой индустрии; провела частичный сбор и анализ научной литературы.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Благодарность

Авторы выражают благодарность редакции Journal of Digital Technologies and Law за помощь в проведении социологического опроса в телеграм-канале журнала https://t.me/JournalDTL

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.41.91 / Авторское право и смежные права в отдельных странах
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 31 октября 2023 г.
Дата одобрения после рецензирования – 20 ноября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.39

Copyrights to the Results of Artificial Intelligence Activity and Means of Their Protection

Dmitriy A. Kazantsev

B2B-Center
Moscow, Russian Federation

Keywords

artificial intelligence,
creativity,
delictual dispositive capacity,
digital technologies,
intellectual property,
law,
legal capacity,
legal personality,
neuron network,
robot

Abstract

Objective: to substantiate the mechanisms of legal protection of intellectual property objects created with the use of artificial intelligence.

Methods: the use of artificial intelligence to create works that are traditionally considered copyright objects was investigated with a set of general scientific and theoretical-legal methods of scientific cognition, including comparison, analogy and synthesis. In addition, the practice of using artificial intelligence, including neural networks, to create such works was considered in several aspects on the basis of retrospective and multifactor analysis.

Results: the paper summarizes the current practice of using artificial intelligence to create works that traditionally belong to intellectual property objects (texts, images, music, software), taking into account the formulated scientific and legal positions. Several qualitatively different variants of the use of artificial intelligence were identified. For each of these variants the mechanism of legal protection was proposed and the areas of their effective application were indicated. Proposals were made to regulate the legal protection of the results of artificial intelligence activity; this was made not in the paradigm of competing doctrines, but by combining several tools, each of them to be applied in a relevant situation.

Scientific novelty: the paper presents ontological differentiation of the results of artificial intelligence activity and the corresponding mechanisms of their legal protection. The author propose to consider the results of activity created by artificial intelligence not as a single object of legal regulation, but as a set of externally similar, but ontologically different objects, each requiring a separate approach to legal protection.

Practical significance: the ontological differentiation of the results of artificial intelligence activity and their corresponding legal protection mechanisms proposed in this paper is relevant both as a basis for further research and as proposals to supplement civil legislation.

For citation

Kazantsev, D. A. (2023). Copyrights to the results of artificial intelligence activity and means of their protection. *Journal of Digital Technologies and Law, 1*(4), 909–931. https://doi.org/10.21202/jdtl.2023.39

Contents

Introduction

Digital technologies are an important factor of the present and a key component of the future. Today, it is appropriate to speak not just about experiments on the introduction of artificial intelligence and big data processing algorithms, but about a consensus on the need for such innovations. The Strategy for the development of information society, approved by the Decree of the President of the Russian Federation No. 203 on May 9, 2017, emphasizes that the competitive advantage in the global market belongs to the states whose industries are based on technologies for analyzing large amounts of data[1]. It is hard to argue with the above thesis: every year economic practice more and more clearly demonstrates the competitive advantages of robotization and the use of artificial intelligence.

The spread of digital technologies in general and the use of artificial intelligence in particular are transforming creative reality, among other things. Various technologies based on big data processing and machine learning have moved from the realm

[1] Decree of the President of the Russian Federation No. 203 of 09.05.2017. (2017). Collection of legislation of the Russian Federation, 20, Art. 2901.

of experimentation to the realm of economic and even household applications. Simply put, with the help of artificial intelligence, any person with basic knowledge of information technologies can not only receive information, but also create it.

Objects like texts, images and musical pieces have traditionally been considered intellectual property. However, today they are created using artificial intelligence. This means that not only in the abstract philosophical discourse, but also in the applied legal sense the following questions become relevant:

1. Should a work created by artificial intelligence be considered a result of creative activity?
2. Is such a work an object of copyright?
3. Is such a work an object of intellectual property?

These questions are related to one another, but each of them characterizes a separate phenomenon of the legal order. Their relevance is conditioned not only by the innovative nature of the technologies to be analyzed to obtain a correct answer to these questions, but also by the ubiquity of such technologies.

Therefore, we should clarify whether today's technologies allow recognizing artificial intelligence as a legal subject. A related but separate issue is the problem of recognizing artificial intelligence as the author of a work of art. The combination of these fundamental legal positions with the answers to the above mentioned questions creates the basis for legal regulation of the results of artificial intelligence activity, which is not only possible, but also necessary today. At the same time, it is important to remember that proper and effective regulation is only possible when the regulatory norms adequately reflect the essence of the regulated objects.

Consequently, for a symmetrical answer to the question about the possibility of a copyright to the results of artificial intelligence activity, it is necessary to analyze the essence of such activity. Actually, this topic cannot be fully disclosed exclusively in the legal field and requires an interdisciplinary approach. Although this research deals only with the regulatory aspect of the problem, we cannot avoid references to, at least, the basic technological aspects and principles of artificial intelligence when formulating legal positions.

Consistent answers to the questions proposed above should take into account the lack of consensus in the academic community on two issues: the essence of cognitive activity of artificial intelligence and its legal personality.

It should be noted, first of all, that the article leaves outside its scope the issues related to the legal personality of artificial intelligence, such as the status of a robot driver and the distribution and implementation of liability for the harm caused by it. Special studies are devoted to these issues, which mainly tend to the conclusion about subsidiary liability (Duffy & Hopkins, 2017), or, more precisely, about the liability matrix, on the basis of which the question of imposing adverse legal consequences is decided individually in each case, taking into account a set of facts (Colonna, 2012).

The mention of automated driving brings us back to the more general question of liability for harm resulting from the work of artificial intelligence (Bertolini, 2013). Today, the question

of the tortability of artificial intelligence seems to be rather practical than legal, because so far the intentional or at least negligent fault of "artificial intelligence intermediaries (developers and users) in the case of harm caused by the artificial intelligence system may be quite probable, legally and expertly provable" (Bertolini, 2013).

A question of even higher order is who becomes a party not only in tort, but also in any legal relationship generated by the actions of artificial intelligence. For example, if the consequences of the actions of artificial intelligence led to the legal existence of a new contract, who exactly will be considered parties to such a contract?

This level of generalization brings us to the question directly related to the topic of this article. Does a robot have legal subjectivity? The issue of copyright on the results of artificial intelligence activity is not reduced to the issue of legal subjectivity, but is directly related to it.

1. Robot as a subject of law

If we recognize artificial intelligence as a subject of law in general, then from this recognition logically follows a positive solution of such issues as the existence of copyright and other intellectual property rights to the works created by it.

However, is it actually – or at least potentially – possible to consider artificial intelligence as a legal subject with inherent rights and obligations? It is not easy to answer this question.

For example, the European Parliament Resolution of February 16, 2017, with recommendations to the Commission on Civil Law Rules on Robotics, while pointing to the increasing relevance of the issue of liability for harm caused by artificial intelligence, notes at the same time that current law does not allow bringing artificial intelligence to liability even when third parties are harmed[2]. Although this Resolution described the prospects for the legal subjectivity of artificial intelligence with utmost caution, the draft of May 31, 2016 formulated several approaches to enshrine "the legal nature of artificial intelligence: to treat it as natural persons, as legal entities, as animals or objects, or to create a new category, with its own characteristics and implications with respect to the attribution of rights and obligations, including liability for damages"[3].

Since the adoption of the resolution, the issue of the legal personality of artificial intelligence has not lost its relevance, and the debate intensifies every year. Somewhat simplifying, in the international discussion we can distinguish several key approaches to resolving this issue: stating that there is no possibility of recognizing the legal personality of artificial intelligence (Calo et al., 2018); applying legal fiction by establishing a legal

---

2 European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

3 Committee on Legal Affairs. (2016, May 31). Draft report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). https://clck.ru/36hAPJ

personality of artificial intelligence similar to that of legal persons (Solaiman, 2017); or even forming a new branch of legislation dedicated to the specific regulation of the status of artificial intelligence and relevant to this specificity (Cofone, 2018).

Noteworthy is the opinion of prominent Russian researchers that today "the most rational, but not uncontroversial, is the use of the concept of the legal personality of artificial intelligence similar to a legal entity or an electronic person; the approach to legal regulation in the framework of legal liability related to users, owners or producers of artificial intelligence systems, rather than related to technological objects" (Ivliev & Egorova, 2022). The concept of "electronic person" as a new subject of law is worth recalling when discussing the issue of intellectual rights to the results of artificial intelligence activities. Here it is also worth noting that the legal personality of artificial intelligence may have similarities with legal personality of a legal entity, but for a number of reasons it cannot be identical to it.

It should be also noted that the question of the legal personality of artificial intelligence cannot be solved once and for all. "What constitutes AI is subjective and best described as moving target. What AI is for one person may not necessarily be AI for another, what was considered AI say fifteen years ago is nowadays considered commonplace and even the question of 'what is intelligence?' is contested and debated" (Greenstein, 2022).

The status of artificial intelligence in legal relations largely depends both on the achieved level of technological development, which allows a robot to perform certain thinking functions, and on the level of social relations development, where the artificial intelligence activity may be more or less significant. From the point of view of the achieved level of technological development to date, "obvious is the failure of the proposal to recognize the legal personality of artificial intelligence similar to that of a physical person, and, despite using the human brain principles to build an artificial intelligence system, the principles of legal regulation of a physical person status cannot be applied to artificial intelligence" (Durneva, 2019).

This is due to the fact that the ability to generate legal relations is only a part of legal personality. A fully-fledged legal subject implements rights and bears responsibilities, as well as becomes liable on the appropriate grounds. The possibility of real application of the same responsibility measures to artificial intelligence today is very doubtful. Not to mention that the category of guilt – be it intention or negligence – does not correlate with the phenomenon of artificial intelligence at all.

Moreover, giving artificial intelligence in its current form a legal personality is a potential threat to the rule of law. After all, legal personality includes the ability to make legally significant decisions. "The threat to the rule of law lies in the fact that most of these decision-making systems are 'black boxes' because they incorporate extremely complex technology that is essentially beyond the cognitive capacities of humans and the law too inhibits transparency to a certain degree. It is here that the demands of the rule of law, such as insight, transparency, fairness and explainability, are almost impossible to achieve,

which in turn raises questions concerning the extent to which the rule of law is a viable concept in the technocratic society" (Greenstein, 2022).

This, in turn, brings us to an aspect that is important for solving the question of the artificial intelligence authorship. Is not it an unjustified anthropomorphization of a robot to mechanistically transfer to artificial intelligence the categories inherent in human consciousness, be it the category of guilt or the category of creativity? We are speaking not about the notorious "uncanny valley effect", but about much more fundamental, ontological aspects.

It should be clearly realized that, anyway, we are discussing the rights of robots from an anthropocentric point of view. This also applies to the axiological dimension, in which we recognize as right and valuable exactly what seems right and valuable to us, humans – even though jurisprudence is called a social-humanitarian discipline, not a natural science, for a reason. The same applies to the utilitarian approach.

Simply put, ultimately we want to give robots legal personality so that they can be answerable to us humans for their actions.

The above-mentioned European Parliament Resolution formulates this idea in a vague and rather ambiguous way: robotics research activities should observe the existing fundamental rights and be performed in the interests of the well-being and self-determination of the individual and society as a whole[4]. The Government of the Russian Federation has formulated a similar idea in the Concept for the regulation of relations in the sphere of artificial intelligence technologies in a more definitive manner: the approach to the regulation of such relations should be based on the principle of balancing the interests of developers, consumers and other persons, as well as defining the boundaries of their responsibility for possible negative consequences of the use of artificial intelligence technologies[5]. Thus, the protection of physical persons, rather than the rights of robots, is at the center.

Even if we recognize as premature the positive resolution of the issue of legal personality of robots, one should agree with the idea "of the need to be proactive and to normatively stipulate the duty of developers and other authorized persons to take all necessary measures to ensure the interests of human beings in the process of artificial intelligence functioning, as well as to develop a system of norms that ensure the fulfillment of this duty" (Durneva, 2019).

The priority of human rights protection when regulating even such a specific sphere as the artificial intelligence activity is important due to one more aspect. The fact that the results of information processing by a robot are comparable, and often even superior to similar

---

4 European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

5 Enactment of the Government of the Russian Federation No. 2129-r of 19.07.2020. Collection of legislation of the Russian Federation. (2020). 35, 5593.

human results, does not mean that the essence of information processing, i. e. thinking, of artificial intelligence is comparable to human thinking. Therefore, there are reasonable doubts that artificial intelligence inherently realizes the value dimension of law.

This is not a question of understanding the value of law as one of the axioms that artificial intelligence may use to process data. It is about realizing this value, i.e. subjective attitude to it. Simply put, does artificial intelligence need rights? From the viewpoint of a developed citizen's logic, the answer is unambiguous: any acting and self-aware subject needs rights. But is this answer so unambiguous from the viewpoint of artificial intelligence? In other words, by assigning rights to a robot, are we not imposing on them a purely alien category that has no value dimension for them?

Within the discussion on the legal personality, legal capacity, and tortability of artificial intelligence, it is necessary to at least point out such an important aspect as self-identification as a subject of law. After all, self-identification is by no means identical to the answer "I am a subject of law" pre-recorded and predetermined by an algorithm. Such an answer can technically be voiced by any smart speaker today. But can we be sure that the meaning behind these words is of any significance for the artificial intelligence making decisions?

In the future, we cannot absolutely exclude the emergence of a real need to recognize and regulate the artificial intelligence's rights to the works created by it. However, it is no less likely, even in the long term, that alternative options will be found for registering and protecting a sustainable link between artificial intelligence and results of its activity, since law is an extremely significant, but not the only institution for regulating relations. It seems that the search for a regulatory institution ontologically relevant to the artificial intelligence phenomenon will become an urgent issue in the nearest future.

These basic considerations regarding legal subjectivity are extremely important for the accurate consideration of the issue of artificial intelligence's copyright to the works created by it.

2. Robot as an instrument of creativity

A robot composes music. A robot draws pictures. A robot writes stories. Lastly, a robot writes a program code. It often makes all of these things not worse than a human being, and it certainly makes them much faster.

It is tempting to equate the creation of works that traditionally belong to the objects of copyright with creativity. In the legal sphere, the question is raised about recognizing artificial intelligence as a copyright holder (Abbott, 2016), because the creative contribution to a piece of work is traditionally regarded as a key attribute of authorship. By and large, the discussion continues about the correctness of indicating the artificial intelligence authorship of the work created with its participation.

Noteworthy in this context is the famous case of Dr. Steven Thaler, which was considered by courts in several common law countries. He claimed to have created an invention machine. This machine developed several useful models, which Dr. Thaler decided to patent. He marked himself as the patentee on the basis that the inventions were made by a machine that belonged to him.

The UK Patent Office refused to register this right, and the inventor appealed against this refusal in court. According to him, the current legislation on copyright protection does not contain a provision that the inventor's rights must belong to a person. He justified the ownership of patent rights to the machine owner by analogy to the rule of property accretion: "The crop belongs to the herd owner".

The case Thaler v. Comptroller-General for Patents, Trademarks and Industrial Designs reached the Court of Appeal of England and Wales, which on September 21, 2021, issued a verdict that the current patent law does not allow considering artificial intelligence as the author of the invention[6]. However, when Thaler sued the local patent office in an Australian court, the judge upheld his position that artificial intelligence can and should be recognized as an inventor[7], and that without granting legal protection to artificial intelligence inventions, the very objective of patent law to promote technological progress would not be achieved.

This dispute demonstrates that a seemingly theoretical question of the artificial intelligence authorship breaks down into two applied questions:

1. Can artificial intelligence be considered the author of an invention, artwork, etc.?

2. If artificial intelligence cannot be considered an author, is such a work subject to copyright protection?

To answer both questions, it is appropriate to continue our review of common law precedents by recalling an age-old case Burrow-Giles Lithographic Co. v. Sarony. On March 17, 1884, the Supreme Court of the United States, in a decision in that case, recognized that the copyright to a photographic card belonged not to a camera or its manufacturer, but to the photographer[8].

We cannot today reliably judge whether, in the last quarter of the 19th century, a camera seemed a futuristic technology to the same extent that artificial intelligence seems in the first quarter of the 21st century. But it is extremely relevant to the court's conclusion that it was the photographer who conceived, organized the execution of, and implemented the creative intent.

Indeed, a photographer is not identical to an artist – but this does not prevent them from both being authors. A composer can create music with a synthesizer, but she is the

---

6 Judgment of the Court of Appeal in England and Wales in Thaler vs Comptroller-General of Patents, Designs and Trademarks [2021] EWCA Civ. 1374. https://clck.ru/36hASY

7 Judgment the Federal Court of Australia in Thaler v. Commissioner of Patents [2021] FCA 879. https://clck.ru/36hAT8

8 Burrow-Giles Lithographic Co. v. Sarony.March 17, 1884. https://clck.ru/36hATk

author of that music. No one doubts that in the first case it is only a method of imaging, and in the second case it is only a method of sound production, and not the transfer of part of the creative work to the instrument.

Moreover, the less work of the author is spent on preparing paints and easel or organizing a brass band, the more the essence of this work constitutes creativity per se. An idea, a creative conception, a vision – this is what the author works with, as their labor is purified from the craft component.

Artificial intelligence in this context appears to be a tool like a camera. The only difference is that this tool gives an artist even more space for creativity. This said, the creation of works of art with the help of artificial intelligence will not cancel or replace painting or photography, just as book printing did not cancel calligraphy.

As long as it is humans, not artificial intelligence, who set the parameters of future works, "it is debatable to recognize copyright of artificial intelligence. Copyright may belong to the user of artificial intelligence, i. e. the creator of the work through artificial intelligence systems. It is unlawful to equate an artificial intelligence system and a human being in rights" (Ivliev & Egorova, 2022). Parameters set by a human by entering a request into a chat or otherwise interacting with artificial intelligence directly affect both the content and quality of the work. It is impossible to paint pictures with the help of a neural network or write texts with the help of a chat room without an initial creative impulse.

Thus, no legal fiction is required to recognize that the author of a work created with the use of artificial intelligence is the person whose creative idea was embodied by that work.

In this context, we consider outdated the legal position that the results of the work of artificial intelligence are not protectable as intellectual property at all, on the grounds that they are not created by humans. For example, in the United States, for theological and ethical reasons, the very possibility of creativity is recognized only for human beings and cannot be recognized for any other subject – neither nature, nor animals, nor machines (Solum, 1992). In this paradigm, a painting created by a neural network is not subject to legal protection to the same extent as a frost drawing on glass or a cat's paw print on canvas.

Plenum of the Supreme Court of the Russian Federation in para. 80 of the Resolution "On application of part 4 of the Civil Code of the Russian Federation" is guided by the same logic: "In resolving the issue of attributing a particular result of intellectual activity to copyright objects, courts should take into account that, within the meaning of Articles 1228, 1257 and 1259 of the Civil Code of the Russian Federation (further – CC RF) in their interrelation, only the result that is created by creative labor can be considered as such. <...> The results created with the help of technical means in the absence of the creative nature of human activity (for example, photo and video recordings by an automatic video surveillance camera used to record administrative offenses) are not considered objects of copyright"[9].

[9] Resolution of the Plenum of the Supreme Court of the Russian Federation No. 10 of 23.04.2019. (2019). Bulletin of the Supreme Court of the Russian Federation, 7.

However, while a surveillance camera recording the work of a turnstile actually does not create a copyright object for lack of a creative idea, the above-mentioned neural network pictures or chat texts cannot be created without such an idea. Therefore, the author of such a work can and should be recognized as the person who gave this idea to the artificial intelligence. We cannot agree with the conclusion that "there is no creativity in the artificial intelligence activity when creating results similar to copyright objects, so the results created by it cannot be qualified as copyright objects and are not subject to protection by intellectual property law" (Vitko, 2019).

"Derivative results of the use of artificial intelligence programs can be recognized as objects of civil law" (Kirsanova, 2022). The rejection of this principle today would mean the denial of legal protection to a huge number of intellectual property objects, which, in turn, would mean an unjustified restriction of copyright of those humans who can and should be recognized as their authors.

Undoubtedly, one may predict future situations in which artificial intelligence creates, on its own initiative, a work "similar to a copyright object"; for example, while executing an algorithm to create design documentation, it may come to a conclusion that the documentation would be incomplete without a five-minute movie about the future object. But today, by their very nature, works created using the artificial intelligence are not just similar to copyright objects but are actually such objects.

Article 1228 CC RF stipulates that creative labor is a factor in the emergence of copyright, while not limiting the legal protection of the results of such labor to its implementation means. Moreover, Article 1227 CC RF directly states that authorship does not depend on the material medium of the work.

This said, the presence of creative labor, resulting in the authorship of an intellectual property object, does not exclude that this object as an artistic work may be secondary in relation to another, previously created piece. At the same time, the very fact of the work's secondary nature cannot and should not exclude the possibility of its legal protection. A good example is: "If a virtual copy (a moving character in a painting) is a new creative object due to certain effects, movements, mimics or other creative actions, it can be recognized as a new derivative object" (Rakhmatulina, 2019). This nuance is important in determining the protectability of works of artificial intelligence, because almost all of them are to some extent based not only on the creative idea of a person who composed the request to artificial intelligence, but also on the processing of an array of previously created works.

Each of the works in that array is a copyright object, even if this right is not commercialized and the works are publicly available without restrictions on reproduction. Moreover, the situation is already relevant when a neural network processes works previously created by other neural networks in order to create a piece of art. Such processing may mean borrowing, more or less noticeable for a human.

In order to avoid disputes about the percentage and substance of borrowing, which are inevitable in case of traditional approaches to copyright protection for the results

of intellectual activity created with the use of artificial intelligence, it seems extremely important to take this nuance into account when characterizing the uniqueness of such works. This uniqueness, as it was said above, is generated not by a neural network processing of other people's works, but by an independent creative impulse that a person as the work author gave to the neural network for its creation.

Nowadays, this impulse, as a rule, is set in the form of a query, which is a combination of key words. To create a finished work of value, a series of queries is usually required. It is this series of queries in combination with the result of their processing by a neural network that represents a unique combination, which in the long run should become the object of intellectual property right to a work created with the use of artificial intelligence. Thus, when identifying a work created by a neural network, it seems reasonable to specify at least the following data:

– the author's name;
– the work title;
– the name of the neural network;
– a sequence of queries given by the author to the neural network.

If this construction is adopted to identify a work created using artificial intelligence, we will have a combination like "Dmitry Kazantsev, painting 'Serenity', generated with the query 'sunset in early autumn in the southern foothills of the Alps' by the Kandinsky neural network". It is reasonable to use such a combination both when indicating authorship of such a work and when registering rights to it in patent institutions if the norms of national legislation provide for such registration for this category of works, for example, if a computer program was created with the help of a neural network.

It is worth recalling that back in 2017 A. Gurko proposed a number of adjustments to the civil legislation for registering intellectual rights to the results of artificial intelligence activities. For example, it was proposed to supplement Article 1228 CC RF with the provisions that the rights to the results of artificial intelligence activities arise in the owner of the hardware-software complex, the right holder of artificial intelligence such as a computer program, or the user of this program. It was proposed to group in a separate article the norms according to which the rights to the works of science, literature and art generated by artificial intelligence belong to the owner of the device used for this objective, and if the device owner is not the owner of the computer program used for this objective, then the rights to such pieces belong to the user of the artificial intelligence (Gurko, 2017).

Over the past few years, the need for some clarification of these novelties has become obvious (e.g., disclosure of the "user" concept regarding the correlation between user rights and holder rights). For example, the following pattern is quite common today: an employer gives a task to an employee – the employee formulates a request for a neural network – the neural network creates a work. It is important to unambiguously and legislatively regulate the issue of who is the right holder in this case. The general

thesis that the rights to the results of artificial intelligence work are held by its user is a simplification in this case and needs to be specified. At the same time, it is obvious that the work created with the participation of artificial intelligence should have legal protection in this case too.

We consider very relevant the central idea that it is logical to grant legal protection to the results of the work of artificial intelligence – including in the form of artistic works, inventions, utility models, computer programs and other copyright objects – as intellectual property of a particular individual or legal entity.

At the same time, the use of such an innovative and specific tool as artificial intelligence requires logically and terminologically distinguishing the works created with its help. The terms "digital" or "algorithmic" (Mazzone & Elgammal, 2019) art, for example, seem to be appropriate. As a generic definition, the concept of "results of artificial intelligence activity" is more or less universally used.

It is important to distinguish between the notions of "results of artificial intelligence activity" and "works of artificial intelligence": in the first case we are talking about the use of artificial intelligence as a tool, which is correct, while in the second case we can assume the creative subjectivity of artificial intelligence, which is premature at present, given the existing technologies. International studies question the correctness of the very naming of neural networks as full-fledged artificial intelligence and recognition of the possibility of their full-fledged thinking and solving creative problems (Lee et al., 2021). Indeed, however vast the information processing capabilities, the results of artificial intelligence activity are reduced, in fact, not to the creation of new works, but to a deep compilation of previously created works.

Speaking about the a priori secondary character of such results in relation to previously created works, one cannot avoid the question of the limits of using those previously created works when working with the result of artificial intelligence activity. The resolution of this issue is beyond the scope of this article, but it seems necessary to state it. For example, in 2023, short videos created by a neural network became viral, in which the characters of iconic works of fiction were presented in an unusual style – from the aura of traditional families in Naples to the Tarkovsky's films settings.

It is obvious that such works are of interest for a consumer not only and not so much due to the original idea of an unusual combination set to the neural network, but due to the use of popular images for this combination. In case of commercialization of such results of artificial intelligence activity, the question will inevitably arise concerning the admissibility of using other people's images with recognized commercial value to create other works, even those using artificial intelligence. It seems that today the solution to this issue, at least at the conceptual level, can be based on the existing approaches and norms of intellectual property protection.

3. Robot as a subject of creativity

Today, legal subjectivity in the creation of works and copyright even to works created with the use of artificial intelligence are human prerogatives. But even postulating this approach as a rule, can we be sure that exceptions to this rule will not occur? One should not limit oneself to today's realities and completely exclude the possibility of a situation in which artificial intelligence will be the actual author of an image, a piece of art, a melody or a computer program.

Technically, even today such a situation can be imagined in at least two cases.

First, when the human formulation of a task for artificial intelligence is so general that it does not allow recognizing the presence of a creative idea ("write a cheerful melody", "make a beautiful pattern in oriental style"). Obviously, identical requests like those can be generated almost simultaneously by a large number of users, which makes it extremely difficult to recognize the author's priority for one of them.

Second, today it is easy to imagine a situation when a robot creates an object which can be legally protected as intellectual property without any direct guidance from a human being. For example, a human gives a task to write technical documentation (the authorship of which can be recognized as human if the above assumptions are accepted), and the artificial intelligence writes a script for calculating risks as a supplement to such documentation (the latter software created by artificial intelligence can hardly be recognized as human authorship due to the absence of any creative intent on the part of the human).

In the following section we will speak not about the works created with the use of artificial intelligence in general, but about those results of artificial intelligence work, in the creation of which the role of human creative participation is vanishingly small or it is difficult to identify such participation at all. Since the results of intellectual activity of artificial intelligence can potentially be created without human creative participation, the following important questions arise when discussing the status of such specific works:

1. Who is the author of the work created by artificial intelligence without human creative participation?

2. Are such results of artificial intelligence activity subject to legal protection?

The simplest answer to these questions may seem to be the recognition that all rights to such a work belong to the artificial intelligence. However, returning to the question of the legal subjectivity of artificial intelligence, we must remember that such a simple, at first glance, solution "implies not only the recognition that the neural network has created an original work, but also that it is able to make conscious decisions on the disposal of rights to it" (Kodaneva, 2021).

Under these circumstances, one may propose to indicate the authorship of artificial intelligence in the work title, but at the same time not to consider artificial intelligence as the author and right holder of the work in the civil-legal sense.

When addressing the issue of legal protection of the results of artificial intelligence activities, it is worth understanding clearly that the rights to works are not limited to the right to indicate authorship. Moreover, it was fairly noted that "the authorship of the result of intellectual activity may have value as a title (the inventor of penicillin, the author of 'War and Peace', etc.), but it is the exclusive rights that are of commercial interest" (Petrakov & Tumakov, 2022).

Indeed, in addition to the right to indicate authorship, there are – in some cases having obvious applied and commercial value – such rights to the results of intellectual activity as "the right to inviolability of the work, the right to promulgation, the right to recall, the right to inviolability of performance); and other rights (for example, the right of succession, the right of access, the right to remuneration for the official result of intellectual activity, the right to protect the phonogram from distortion in its use, the right to obtain a patent, etc.)"[10].

Both the wording of civil law norms, legal doctrine and the practice of intellectual property protection tell us that one person may be considered the author of a work, but another person may have rights to the work, exclusive rights among them. From this we can conclude that the right to indicate authorship is separate from the exclusive rights to the work.

Thus, the absence of copyright on the work created by artificial intelligence – or, if you will, reduction of such rights to the mandatory indication of the fact that this work is the result of the artificial intelligence work – should not mean the absence of legal protection for such a work. The only question is who will be the right holder in this case.

The most obvious option is to consider the results of artificial intelligence activity as a special case of a work for hire, except that the artificial intelligence in place of an employee to whom the employer sets an official task (Yanisky-Ravid, 2017). Indeed, the legal consequences in both cases will be similar: it is not the author of the work who becomes the right holder, but the subject who initiated its creation. However, similarity does not mean identity in this case. For example, artificial intelligence is not in labor relations with its right holder; the request of the right holder is not formalized according to the rules of a work for hire; the request may not include the key parameters of the future work at all, etc.

The question of the difference between a work for hire and a request for a neural network cannot be regarded as exclusively legal and theoretical. Its practical significance is conditioned by the rapid spread of artificial intelligence technologies in industrial sphere. Works created by artificial intelligence within the framework of commercial activities of a legal entity are, perhaps primarily, the very objects of intellectual property, the rights to which have commercial value.

All this forces us to address not from a theoretical, but from a practical viewpoint, the question that "the introduction of the right to the result of artificial intelligence activity

[10] Resolution of the Plenum of the Supreme Court of the Russian Federation No. 10 of 23.04.2019. (2019). Bulletin of the Supreme Court of the Russian Federation, 7.

can be modeled along the pattern of neighboring rights, but it clearly loses its connection with copyright; therefore, we think it appropriate to speak of the sui generis right to digital results of artificial intelligence activity" (Kharitonova, 2019). Indeed, if authorship of the results of artificial intelligence activities cannot be recognized for a particular person or group of persons, the legal protection of such results requires new legal tools. These instruments can and should build on the existing intellectual law constructs, but they cannot be reduced to a single structure.

In this paradigm, it seems reasonable to agree with the thesis of "the existence of prerequisites for the emergence of a new legal institution in intellectual property law – the institution of the right to the results of artificial intelligence activity. The institution is sui generis within the framework of intellectual property law and is not reduced to the traditional copyright, patent law, neighboring rights and others, although in some part it is based on the constructions of such traditional institutions" (Anikin, 2022).

Thus, if a person can be recognized as an author of the results of artificial intelligence activity and, accordingly, artificial intelligence itself can be recognized only as an instrument of implementation of a person's creative idea, then the legal protection of the work can be based on the existing copyright norms. However, if such recognition becomes difficult for one reason or another, a new legal institution will potentially be required in the future. It is important not to regard these two approaches as competing. After all, it is only on their combination and the application of each in a relevant situation that the future right to the results of artificial intelligence should be based.

Conclusions

When formulating conclusions regarding the legal regulation and legal protection of the results of artificial intelligence activity, it is necessary, first of all, to realize that this field is elastic to a certain extent. The results that are relevant today must be regularly verified in the future according to the achieved level of technology.

However, today, when regulating copyrights to texts, images, musical pieces and other works created with the use of artificial intelligence, it is rational to proceed first of all from the prevalence of the absence of legal subjectivity in artificial intelligence. This does not mean that it is fundamentally impossible to recognize artificial intelligence as a legal subject. It only means that today, both from the viewpoint of existing digital technologies and from the viewpoint of legal consciousness, delictual dispositive capacity and other legal institutions, it is at least doubtful that a robot can implement its legal subjectivity.

"Giving robots (an artificial intelligence system) the status of a legal subject will not entail any explicit negative consequences in the foreseeable future. At the same time, the advantages of such a solution are also not visible, compared to considering robots

(artificial intelligence systems) as quasi-subjects of law. Proceeding from the Occam's philosophical principle of not to multiply entities unless absolutely necessary, we believe it premature to introduce such a fundamentally new legal subject as a robot (an artificial intelligence system) into the legal sphere" (Channov, 2022).

Performance of intellectual and creative tasks by a robot at a level comparable and sometimes even superior to that of a human being cannot be considered as a basis for recognizing artificial intelligence as identical to a human being, both in terms of law in general and copyright in particular. "There is no doubt that the gap between artificial intelligence and humans is narrowing. However, it does not seem likely to be completely bridged any time soon, as it is humans that customize models, select training examples, and use digital technologies for creativity. The idea that machines can be artists or can even replace artists, as they have already replaced some professions, seems too bold so far"[11]. At the same time, the sphere of creativity by virtue of its very specificity dictates caution in the aspect of transferring anthropomorphic features to artificial intelligence, including assigning it the category of creativity.

"Attributing legal subjectivity to artificial intelligence would help to deal with the problem of authorship. However, this approach seems unsuitable for solving other important problems, such as liability. We believe that nothing will be achieved in terms of the copyright provisions, since everything is created by a human being with their creativity, unique and new ideas. This can be achieved even now by rethinking the doctrinal aspects that shape copyright, such as uniqueness and creativity, and identifying the 'decisive' person behind works of art created with the help of artificial intelligence" (Sushkova, 2022). It is the creative intent of a person, and not at all the tool for the implementation of such an intent, that should be the criterion of authorship.

To date, based on these assumptions, the main conclusions regarding intellectual rights to the results of artificial intelligence activity can be formulated in the form of several basic theses.

First, it seems premature to give artificial intelligence a legal subjectivity, including due to the obvious problems with the awareness and implementation of its legal capacity, as well as with the practical implementation of its delictual capacity.

Second, today's practice of using artificial intelligence to create texts, musical works, images, software and other copyright objects in most cases allows identifying the person or group of persons whose creative intent was implemented by artificial intelligence. In these circumstances, the recognition of artificial intelligence as the author of a work seems unreasonable.

[11] Suetin, N. (2020, June 8). Artificial intelligence in modern art. Skolkovo innovative center. https://clck.ru/Ntrio

Third, the refusal to recognize artificial intelligence as the author of a work should not be followed by a refusal to legally protect such a work. As a general rule, it is the person whose creative idea was implemented with the use of artificial intelligence that would be recognized as the author and right holder. In this sense, the use of artificial intelligence for creativity is in essence differs little from the use of other technical means for the same objectives, such as a camera, synthesizer, etc.

Fourth, the absence of ontological difference between artificial intelligence and a camera in the context of creativity does not mean that there is no actual difference. In this regard, it is relevant to use special concepts for the results of creativity in which artificial intelligence was involved. This could be a general notion of "the results of artificial intelligence activity" or more specific definitions such as "digital art".

Fifth, when it is impossible to identify the creative intent of a human being in the creation of a work by artificial intelligence and the actual author of the work is artificial intelligence, it deserves a special designation as a work of artificial intelligence. Such designation replaces the indication of authorship in the civil-legal sense, and such works are subject to legal protection under special rules. These rules, in particular, provide for the absence of indication of the author's name and legal protection of the work as intellectual property of the owner of artificial intelligence. The mechanism of legal protection of the results of the artificial intelligence work in this case may be similar, but not identical, to that of a work for hire.

Finally, it is important to take into account the principles and fundamentals of the technology of information processing by artificial intelligence – in particular, the fact that in the works formed by it, there are inevitable repetitions of elements of already existing works, including those created by artificial intelligence. Together with the postulation of authorship of the person who provided the artificial intelligence with the key words to create the work, it seems necessary to take into account in legal reality the specificity of the copyright object created with the use of artificial intelligence, namely: the legal protection object is a combination of the work per se (text, melody, image, etc.) generated by artificial intelligence, and the key words set by the author for such generation. The object of copyright protection in this case will be a unique combination of the author's name, the sequence of their requests to the artificial intelligence and the work per se, formed by the artificial intelligence as a result of processing the sequence of these requests.

The combination of these approaches will help not only to develop an adequate regulation of the results of artificial intelligence activity, but also to make such results a full-fledged element of the legal domain and in this sense a full-fledged intellectual property. Since legal protection is an important factor of interest and investment, which is clearly demonstrated by patent law, for example, one should hope that circumspect legal regulation of intellectual rights to works created with the participation of artificial intelligence will serve as an impetus for progress in this area.

References

Abbott, R. (2016). I Think, Therefore I Invent: Creative Computers and the Future of Patent Law. *Boston College Law Review*, *57*. https://doi.org/10.2139/ssrn.2727884

Anikin, A. S. (2022). On the protectability of the results of artificial intelligence activity as an object of intellectual property. *Civilist*, *2*, 25–31. (In Russ.).

Bertolini, A. (2013). Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules. *Law, Innovation and Technology*, *5*(2), 214–247. https://doi.org/10.5235/17579961.5.2.214

Calo, R., Chizeck, H. J., Joh, E., & Hannaford, B. (2018). Panel 2: Accountability for the Actions of Robots. *Seattle University Law Review*, *41*, 1101. https://clck.ru/36pgAM

Cofone, I. (2018). Servers and Waiters: What Matters in the Law of AI. *Stanford Technology Law Review*, *21*, 167. https://doi.org/10.31228/osf.io/2nstf

Channov, S. E. (2022). Robot (Artificial Intelligence System) as a Subject (Quasi-Subject) of Law. *Actual Problems of Russian Law*, *12*. (In Russ.). https://doi.org/10.17803/1994-1471.2022.145.12.094-109

Colonna, K. (2012). Autonomous Cars and Tort Liability. *Case Western Reserve Journal of Law, Technology & the Internet*, *4*(4). https://doi.org/10.2139/ssrn.2325879

Duffy, S. H., & Hopkins, J. P. (2017). Sit, Stay, Drive: The Future of Autonomous Car Liability. *SMU Science & Technology Law Review*, *16*(3), 453–480. https://clck.ru/36pgCG

Durneva, P. N. (2019). Artificial Intelligence: An Analysis from the Standpoint of the Classical Legal Capacity Theory. *Civil law*, *5*. (In Russ.). https://doi.org/10.18572/2070-2140-2019-5-30-33

Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, *30*, 291–323. https://doi.org/10.1007/s10506-021-09294-4

Gurko, A. (2017). Artificial intelligence and copyright law: a glance into the future. *Intellectual Property*, *12*.

Ivliev, G. P., & Egorova, M. A. (2022). Legal Issues of the Legal Status of Artificial Intelligence and Products Created by Artificial Intelligence Systems. *Journal of Russian Law*, *6*, 32–46. (In Russ.). https://doi.org/10.12737/jrl.2022.060

Kharitonova, Yu. S. (2019). legal regime of the results of artificial intelligence functioning. In E. B. Lauts (Ed.), *Modern information technologies and law* (pp. 68–82). Moscow: Statut. (In Russ.).

Kirsanova, E. E. (2022). *Legal regulation of the turnover of right to the results of intellectual activity in digital economy*. Moscow: Yustitsinform.

Kodaneva, S. I. (2021). Transformation of copyright under the development of digital technologies. *Law and Digital Economy*, *4*(14). (In Russ.). https://doi.org/10.17803/2618-8198.2021.14.4.031-038

Lee, J-.A., Hilty, R., & Liu, K-.C. (Eds.). (2021). *Artificial intelligence and intellectual property.* Oxford University Press. https://doi.org/10.1093/oso/9780198870944.001.0001

Mazzone, M., & Elgammal, A. (2019). Art, Creativity, and the Potential of Artificial Intelligence. *Arts*, *8*(1). https://doi.org/10.3390/arts8010026

Petrakov, N. A., & Tumakov, A. V. (2022). The problems of legal protection of objects created with the use of artificial intelligence technologies. *Civilist*, *4*. (In Russ.).

Rakhmatulina, R. Sh. (2019). Electronic Form of copyright Items. *Law and Digital Economy*, *1*. (In Russ.). https://doi.org/10.17803/2618-8198.2019.03.1.035-038

Solaiman, S. M. (2017). Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy. *Artificial Intelligence and Law*, *25*. https://doi.org/10.1007/s10506-016-9192-3

Solum, L. B. (1992). Legal Personhood for Artificial Intelligences. *North Carolina Law Review*, *70*(4), 1231–1287. http://scholarship.law.unc.edu/nclr/vol70/iss4/4

Sushkova, O. V. (2022). Legal Means of Circulation of Objects Created with the Use of Artificial Intelligence Technologies. *Civil Law*, *2*. (In Russ.). https://doi.org/10.18572/2070-2140-2022-2-12-15

Vitko, V. (2019). Analysis of scientific views of authorship and right for results of ai activity (continued). *Intellectual Property*, *3*, 5–22. (In Russ.).

Yanisky-Ravid, Sh. (2017). Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era – the HumanLike Authors Are Already Here – a New Model. *Michigan State Law Review*, *4*. https://doi.org/10.2139/ssrn.2957722

Author information

Dmitriy A. Kazantsev – Cand. Sci. (Law), Head of the Department of normative-legal regulation of the B2B-Center electronic trading platform operator
Address: 18/22 3rd Rybiskaya Str., 107113 Moscow, Russian Federation
E-mail: info@dkazantsev.ru
ORCID ID: https://orcid.org/0000-0003-2182-5776
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1149755

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – May 15, 2023
Date of approval – July 15, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:34.096:347.211:004.8
EDN: https://elibrary.ru/phbnki
DOI: https://doi.org/10.21202/jdtl.2023.39

Авторские права на результаты деятельности искусственного интеллекта и способы их защиты

Дмитрий Александрович Казанцев

B2B-Center
г. Москва, Российская Федерация

Ключевые слова

деликтоспособность,
интеллектуальная собственность,
искусственный интеллект,
нейросеть,
право,
правоспособность,
правосубъектность,
робот,
творчество,
цифровые технологии

Аннотация

Цель: обоснование механизмов правовой защиты объектов интеллектуальной собственности, созданных с использованием искусственного интеллекта.

Методы: использование искусственного интеллекта для создания произведений, традиционно относящихся к объектам авторского права, исследовалось посредством совокупности общенаучных и теоретико-правовых методов научного познания, включая сравнение, аналогию и синтез. Кроме того, практика использования искусственного интеллекта, в том числе нейросетей, для создания таких произведений была рассмотрена в нескольких аспектах на основе ретроспективного и многофакторного анализа.

Результаты: в работе обобщена актуальная практика использования искусственного интеллекта для создания произведений, традиционно относящихся к объектам интеллектуальной собственности (текстов, изображений, музыки, программ для ЭВМ), с учетом сформулированных научных и правовых позиций. Выделено несколько качественно различающихся между собой вариантов использования искусственного интеллекта. Для каждого из этих вариантов был предложен механизм правовой защиты, а также указаны области эффективного их применения. Даны предложения по регулированию правовой защиты результатов деятельности искусственного интеллекта не в парадигме конкурирующих доктрин, а в сочетании нескольких инструментов с применением каждого из них в релевантной ситуации.

Научная новизна: в работе представлена онтологическая дифференциация результатов деятельности искусственного интеллекта и соответствующих им механизмов правовой защиты. Созданные искусственным интеллектом результаты деятельности предлагается считать не единым объектом правового регулирования, а совокупностью внешне сходных, но онтологически различных объектов, каждый из которых требует собственного подхода к правовой охране.

Практическая значимость: предложенная в настоящей работе онтологическая дифференциация результатов деятельности искусственного интеллекта и соответствующих им механизмов правовой защиты актуальна как в качестве основы для дальнейших исследований, так и в качестве предложений для дополнения норм гражданского законодательства.

Для цитирования

Казанцев, Д. (2023). Авторские права на результаты деятельности искусственного интеллекта и способы их защиты. *Journal of Digital Technologies and Law*, *1*(4), 909–931. https://doi.org/10.21202/jdtl.2023.39

Список литературы

Аникин, А. С. (2022). К вопросу об охраноспособности результатов деятельности искусственного интеллекта как объекта интеллектуальной собственности. *Цивилист*, *2*(38), 25–31. https://www.elibrary.ru/kuiptf

Витко, В. (2019). Анализ научных представлений об авторе и правах на результаты деятельности искусственного интеллекта. *Интеллектуальная собственность*. *Авторское право и смежные права*, *3*, 5–22. https://www.elibrary.ru/jsfbce

Гурко, А. (2017). Искусственный интеллект и авторское право: взгляд в будущее. *Интеллектуальная собственность*. *Авторское право и смежные права*, *12*, 7–18. https://www.elibrary.ru/zukikl

Дурнева, П. Н. (2019). Искусственный интеллект: анализ с точки зрения классической теории правосубъектности. *Гражданское право*, *5*. https://doi.org/10.18572/2070-2140-2019-5-30-33

Ивлиев, Г. П., Егорова, М. А. (2022). Юридическая проблематика правового статуса искусственного интеллекта и продуктов, созданных системами искусственного интеллекта. *Журнал российского права*, *6*, 32–46. https://doi.org/10.12737/jrl.2022.060

Кирсанова, Е. Е. (2022). *Правовое регулирование оборота прав на результаты интеллектуальной деятельности в цифровой экономике*. Москва: Юстицинформ. https://www.elibrary.ru/rfcgjq

Коданева, С. И. (2021). Трансформация авторского права под влиянием развития цифровых технологий. *Право и цифровая экономика*, *4*(14). https://doi.org/10.17803/2618-8198.2021.14.4.031-038

Петраков, Н. А., Тумаков, А. В. (2022). Проблемы правовой охраны объектов, созданных с использованием технологий искусственного интеллекта. *Цивилист*, *4*(40), 16–18. https://www.elibrary.ru/wtcbcj

Рахматулина, Р. Ш. (2019). Цифровая форма объектов авторского права. *Право и цифровая экономика*, *1*. https://doi.org/10.17803/2618-8198.2019.03.1.035-038

Сушкова, О. В. (2022). Правовые средства оборота объектов, созданных с использованием технологий искусственного интеллекта. *Гражданское право*, *2*. https://doi.org/10.18572/2070-2140-2022-2-12-15

Харитонова, Ю. С. (2019). Правовой режим результатов деятельности искусственного интеллекта. В кн. Е. Б. Лаутс (отв. ред.), *Современные информационные технологии и право*, 68–83. Москва: Статут.

Чаннов, С. Е. (2022). Робот (система искусственного интеллекта) как субъект (квазисубъект) права. *Актуальные проблемы российского права*, *12*. https://doi.org/10.17803/1994-1471.2022.145.12.094-109

Abbott, R. (2016). I Think, Therefore I Invent: Creative Computers and the Future of Patent Law. *Boston College Law Review*, *57*. https://doi.org/10.2139/ssrn.2727884

Bertolini, A. (2013). Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules. *Law, Innovation and Technology*, *5*(2), 214–247. https://doi.org/10.5235/17579961.5.2.214

Calo, R., Chizeck, H. J., Joh, E., & Hannaford, B. (2018). Panel 2: Accountability for the Actions of Robots. *Seattle University Law Review*, *41*, 1101. https://digitalcommons.law.uw.edu/faculty-articles/493

Cofone, I. (2018). Servers and Waiters: What Matters in the Law of AI. *Stanford Technology Law Review*, *21*, 167. https://doi.org/10.31228/osf.io/2nstf

Colonna, K. (2012). Autonomous Cars and Tort Liability. *Case Western Reserve Journal of Law, Technology & the Internet*, *4*(4). https://doi.org/10.2139/ssrn.2325879

Duffy, S. H., & Hopkins, J. P. (2017). Sit, Stay, Drive: The Future of Autonomous Car Liability. *SMU Science & Technology Law Review*, *16*(3), 453–480. https://scholar.smu.edu/scitech/vol16/iss3/4

Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, *30*, 291–323. https://doi.org/10.1007/s10506-021-09294-4

Lee, J-.A., Hilty, R., & Liu, K-.C. (Eds.). (2021). *Artificial intelligence and intellectual property.* Oxford University Press. https://doi.org/10.1093/oso/9780198870944.001.0001

Mazzone, M., & Elgammal, A. (2019). Art, Creativity, and the Potential of Artificial Intelligence. *Arts*, *8*(1). https://doi.org/10.3390/arts8010026

Solaiman, S. M. (2017). Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy. *Artificial Intelligence and Law*, *25*. https://doi.org/10.1007/s10506-016-9192-3

Solum, L. B. (1992). Legal Personhood for Artificial Intelligences. *North Carolina Law Review*, *70*(4), 1231–1287. http://scholarship.law.unc.edu/nclr/vol70/iss4/4

Yanisky-Ravid, Sh. (2017). Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era – the HumanLike Authors Are Already Here – a New Model. *Michigan State Law Review*, 4. https://doi.org/10.2139/ssrn.2957722

Сведения об авторе

Казанцев Дмитрий Александрович – кандидат юридических наук, руководитель Департамента нормативно-правового регулирования оператора электронной торговой площадки B2B-Center (АО «Центр развития экономики»)
Адрес: 107113, Российская Федерация, г. Москва, 3-я Рыбинская улица, 18/22
E-mail: info@dkazantsev.ru
ORCID ID: https://orcid.org/0000-0003-2182-5776
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1149755

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.41.51 / Охрана авторских прав
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 15 мая 2023 г.
Дата одобрения после рецензирования – 15 июля 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.40

Artificial Intelligence Impact on the Environment: Hidden Ecological Costs and Ethical-Legal Issues

Alesia Zhuk

University Pompeu Fabra
Barcelona, Spain

Keywords

algorithmic bias,
artificial intelligence,
data center,
digital technologies,
ecological costs,
electronic waste,
energy consumption,
law,
natural ecosystems,
sustainability

Abstract

Objective: to identify the hidden ecological costs associated with the elaboration, implementation and development of artificial intelligence technologies, in order to ensure its sustainable and harmonious integration with various economic sectors by identifying optimal moral-ethical and political-legal strategies.

Methods: the conducted research is based on an ecological approach to the development and implementation of artificial intelligence, as well as on an interdisciplinary and political-legal analysis of ecological problems and risks of algorithmic bias, errors in artificial intelligence algorithms and decision-making processes that may exacerbate environmental inequalities and injustice towards the environment. In addition, analysis was performed in regard to the consequences of natural ecosystems destruction caused by the development of artificial intelligence technologies due to the computing energy-intensiveness, the growing impact of data centers on energy consumption and problems with their cooling, the electronic waste formation due to the rapid improvement of equipment, etc.

Results: the analysis shows a range of environmental, ethical and political-legal issues associated with the training, use and development of artificial intelligence, which consumes a significant amount of energy (mainly from non-renewable sources). This leads to an increase in carbon emissions and creates obstacles to further sustainable ecological development. Improper disposal of artificial intelligence equipment exacerbates the problem of e-waste and pollution of the planet, further damaging the environment.

Errors in artificial intelligence algorithms and decision-making processes lead to environmental injustice and inequality. AI technologies may disrupt natural ecosystems, jeopardizing wildlife habitats and migration patterns.

Scientific novelty: the environmental consequences of the artificial intelligence use and further development, as well as the resulting environmental violations and costs of sustainable development, were studied. This leads to the scientific search for optimal strategies to minimize environmental damage, in which legal scholars and lawyers will have to determine ethical-legal and political-legal solutions at the national and supranational levels.

Practical significance: understanding the environmental impact of AI is crucial for policy makers, lawyers, researchers, and industry experts in developing strategies to minimize environmental harm. The findings emphasize the importance of implementing energy efficient algorithms, switching to renewable energy sources, adopting responsible e-waste management practices, ensuring fairness in AI decision-making and taking into account ethical considerations and rules of its implementation.

For citation

Zhuk, A. (2023). Artificial Intelligence Impact on the Environment: Hidden Ecological Costs and Ethical-Legal Issues. *Journal of Digital Technologies and Law, 1*(4), 932–954. https://doi.org/10.21202/jdtl.2023.40

Contents

Introduction

Artificial intelligence (AI) has emerged as a powerful and transformative force, revolutionising various aspects of human lives, from healthcare to transportation, and from customer service to financial systems. With its ability to process vast amounts of data and learn from patterns, AI has opened up new frontiers of innovation and efficiency. However, as society marvels at the advancements brought by AI, it becomes crucial to recognise and examine the hidden ecological cost associated with this technological revolution.

As the demand for AI applications grows, the energy consumption required to power the computational infrastructure also increases. According to a study conducted by Strubell et al. (2019), training a single state-of-the-art AI model can emit as much carbon dioxide as the lifetime emissions of five cars. Data centres, which are responsible for housing and running AI systems, contribute significantly to this energy consumption, often relying on non-renewable energy sources. The exponential growth of AI technology raises concerns about the long-term environmental impact, as the environmental cost associated with the AI revolution remains largely unnoticed and unaccounted for.

Moreover, the rapid evolution of AI hardware leads to shorter device lifecycles, resulting in a surge of electronic waste (e-waste). The Global E-waste Monitor 2020 report indicates that e-waste generation reached a record 53.6 million metric tonnes, with only 17.4 % being officially collected and recycled[1]. Improper management of outdated AI hardware components poses significant environmental risks, contributing to pollution and resource depletion.

Whilst AI presents immense potential for environmental monitoring and conservation efforts, its deployment can also disrupt natural ecosystems. Environmental monitoring drones and autonomous vehicles used for resource exploration, for example, have the potential to disturb wildlife habitats, interfere with migration patterns, and exacerbate ecosystem imbalances. The unintended consequences of AI on biodiversity and ecosystems necessitate careful consideration to ensure responsible and sustainable deployment.

In light of these concerns, it becomes essential to delve deeper into the environmental footprint of AI and explore strategies for mitigating its negative ecological impacts. This article will examine various aspects of the ecological cost associated with AI, highlighting the need for energy-efficient algorithms, responsible e-waste management practices, sustainable data centre infrastructure, and ethical considerations in AI

[1] Forti, V., Baldé, C. P., Kuehr, R., & Bel, G. (2020). The global e-waste monitor 2020: Quantities, flows and the circular economy potential. United Nations University (UNU), International Telecommunication Union (ITU) & International Solid Waste Association (ISWA). Bonn; Geneva; Rotterdam.

decision-making. By shedding light on these issues, it aims to foster discussions and actions that lead to a more environmentally conscious approach to AI development and deployment.

1. Energy consumption

As society continues to harness the power of AI, it becomes imperative to acknowledge and tackle the substantial energy consumption that accompanies this technological revolution. This section explores the energy-intensive nature of AI computations, the significant energy demands of data centers, and the concerning reliance on non-renewable energy sources. By shedding light on the hidden ecological costs of the AI revolution, we can gain a deeper understanding of the environmental implications associated with AI's remarkable impact on various domains of human life.

AI computations are known for their substantial energy requirements due to the processing of vast amounts of data and the execution of complex algorithms. Training state-of-the-art AI models, in particular, consumes a significant amount of energy, with large-scale models consuming as much energy as hundreds of megawatt-hours, equivalent to the energy required to power thousands of homes for several months (Strubell et al., 2019). The computational demands and iterative processes involved in training AI models contribute to their high energy consumption. These energy requirements are driven by the need to process large datasets, perform complex matrix operations, and optimise model parameters through multiple iterations. Understanding the energy footprint of AI computations is essential for comprehending the environmental impact associated with their widespread adoption.

Data centers play a vital role in supporting AI systems by housing and running the computational infrastructure. However, they contribute significantly to the overall energy consumption of AI. These facilities require substantial electricity to power servers, cooling systems, and networking equipment. The high-performance computing capabilities necessary for AI computations result in increased energy demands for data centers. Hanus et al. (2023) underscore the energy-intensive nature of data centers and the challenges they face in achieving energy efficiency. The growth of AI technology has led to an increase in the number and size of data centers, amplifying their environmental impact. The inefficient utilisation of computing resources and cooling systems in data centers further exacerbates their energy consumption and environmental footprint.

A pressing concern regarding AI's energy consumption is the reliance on non-renewable energy sources. Conventional power grids, often fueled by fossil fuels, are the primary sources of electricity for AI computations. This reliance on non-renewable energy exacerbates greenhouse gas emissions and environmental challenges. Şerban et al. (2020) stress the

importance of transitioning to renewable energy sources for sustainable AI infrastructure. Incorporating renewable energy solutions, such as solar or wind power, in data centers can reduce the carbon footprint of AI systems and mitigate their environmental impact. The adoption of renewable energy technologies not only reduces greenhouse gas emissions but also promotes the development of a more sustainable energy infrastructure to support the growing demands of AI computations.

1.1. The energy-intensive nature of AI computations

The energy-intensive nature of AI computations has become a growing concern due to the significant energy requirements associated with training and running sophisticated AI models (Henderson et al., 2018). As AI applications continue to advance and become more complex, the demand for computational power has skyrocketed, leading to increased energy consumption.

One primary contributor to the energy consumption of AI computations is the training phase. Training a deep learning model involves feeding vast amounts of data into neural networks, which then adjust their internal parameters through iterative processes to optimise performance. This training process often requires multiple iterations over large datasets, utilising powerful hardware infrastructure such as graphics processing units (GPUs) or specialised tensor processing units (TPUs) (Strubell et al., 2019).

These hardware components are highly energy-intensive, consuming significant amounts of electricity to perform the complex calculations necessary for training AI models. The energy consumption during training can range from several hundred kilowatt-hours (kWh) to several thousand kWh, depending on the size and complexity of the model, the size of the dataset, and the hardware infrastructure used (Schwartz et al., 2020).

For example, a study by Schwartz et al. (2020) estimated that training a single state-of-the-art language model can emit as much carbon dioxide as the lifetime emissions of five cars. This highlights the substantial environmental impact associated with the energy consumption of AI computations.

In addition to the training phase, the deployment and inference of AI models also contribute to energy consumption. Once a model is trained, it needs to be deployed and run on various devices or cloud servers to make predictions or perform specific tasks in real-time. This inference phase also requires computational resources, although typically less intensive compared to training. However, when AI models are deployed at scale, the cumulative energy consumption can still be substantial (Strubell et al., 2019).

The energy-intensive nature of AI computations raises concerns about the environmental impact and sustainability of AI technologies. As AI applications continue to proliferate across industries and sectors, the demand for computational resources will only increase, leading to even higher energy consumption. It becomes crucial to explore energy-efficient

computing architectures, develop algorithms that minimise computational requirements, and adopt renewable energy sources to power AI infrastructure (Ding et al., 2021).

Efforts are underway to address these challenges. Researchers and industry experts are actively working on developing more energy-efficient algorithms and hardware architectures, exploring techniques such as model compression, quantisation, and distributed training. These approaches aim to reduce the computational requirements of AI models without significantly compromising performance (Ding et al., 2021). Furthermore, there is an increasing focus on optimising data centre operations and adopting renewable energy sources to power AI infrastructure, reducing the carbon footprint associated with AI computations (Strubell et al., 2019).

1.2. Data centers: Energy hogs of the AI infrastructure

Data centers play a critical role in supporting the AI infrastructure, serving as the backbone for storing and processing vast amounts of data. However, these data centers are also significant energy consumers, raising concerns about their environmental impact (Dhar, 2020).

Data centers house the servers, networking equipment, and storage systems required to handle the computational demands of AI workloads. These facilities operate around the clock, consuming substantial amounts of electricity for powering and cooling the equipment, as well as providing uninterruptible power supply systems (UPSS) for backup (Shah et al., 2010).

The energy consumption of data centers is driven by various factors, including the number and efficiency of servers, the cooling systems, and the overall infrastructure design. Server racks and cooling equipment consume a significant portion of the energy, with cooling alone accounting for up to 40% of the total energy consumption (Masanet et al., 2020). A study estimated that data centers globally consumed approximately 196 to 400 terawatt-hours (TWh) of electricity in 2020, accounting for about 1 % of the global electricity consumption[2]. The energy efficiency of data centers has become a major focus in reducing their environmental footprint. Efforts are underway to improve server efficiency, optimize cooling systems, and design data centers with energy-efficient principles in mind. Techniques such as server virtualization, advanced cooling technologies, and power management strategies are being implemented to enhance energy efficiency (Shah et al., 2010).

Furthermore, there is a growing interest in adopting renewable energy sources to power data centers. Many companies are investing in renewable energy projects and purchasing renewable energy certificates (RECs) to offset their electricity consumption (Dhar, 2020). For example, Google announced in 2017 that it had achieved a milestone of purchasing

[2] Garcia, C. (2022). The Real Amount of Energy A Data Center Uses. https://clck.ru/36kxEN

enough renewable energy to match 100 % of its global electricity consumption for its data centers and offices[3].

To address the energy challenges posed by data centers, industry collaborations, government regulations, and research initiatives are being established. These efforts aim to develop standards, promote best practices, and encourage the adoption of energy-efficient technologies in data center operations (Shah et al., 2010). In the UK, the Data Centre Alliance is actively working to drive energy efficiency improvements and sustainability in the data center industry[4].

1.3. Non-renewable energy sources and carbon emissions

The reliance of AI infrastructure on non-renewable energy sources has significant implications for carbon emissions and the overall environmental impact. The generation of electricity from fossil fuels, such as coal and natural gas, contributes to greenhouse gas emissions and exacerbates climate change (Ram et al., 2018). In fact, the carbon emissions from data centers alone are estimated to rival those of the aviation industry[5].

Data centers, which house the computational infrastructure for AI, are known to be energy-intensive facilities. They require substantial amounts of electricity to power the servers, cooling systems, and other supporting infrastructure. In many regions, the grid electricity used to power data centers predominantly comes from non-renewable sources. For example, in the United Kingdom, a significant portion of the electricity generation still relies on fossil fuels[6].

The carbon emissions associated with non-renewable energy sources directly contribute to the carbon footprint of AI systems. A study by Rolnick et al. (2022) estimated that training a large AI model can emit as much carbon as an average American car over its entire lifetime.

To address these concerns, there is a growing movement within the AI community to transition towards renewable energy sources and reduce carbon emissions. Several major technology companies, including Microsoft and Amazon, have made commitments to achieve carbon neutrality and rely on renewable energy for their data centers[7].

Moreover, governments and organizations are taking steps to promote the adoption of renewable energy in the AI sector. The European Union, for instance, has set targets

3 Google. (2021). Google reaches 100% renewable energy goal. https://clck.ru/36kxG4

4 Data Centre Alliance. (n.d.). About the DCA. https://clck.ru/36kxHA

5 Lim, S. (2022, July 14). Media industry's pollution equivalent to aviation, study finds. Campaign. https://clck.ru/36kxHu

6 Department for Business, Energy & Industrial Strategy. (2020). BEIS Electricity Generation Costs. https://clck.ru/36kxKS

7 Microsoft. (2022). Microsoft announces plan to be carbon negative by 2030. https://clck.ru/36kxLJ ; See also Amazon. (n.d.). Amazon and Global Optimism announce The Climate Pledge. https://clck.ru/36kxMP

to increase the share of renewable energy and reduce greenhouse gas emissions in its member states[8].

Additionally, research efforts are focused on developing energy-efficient algorithms and hardware designs to minimise energy consumption and carbon emissions during AI computations. Techniques like model compression, quantisation, and specialised hardware architectures are being explored to optimise the energy efficiency of AI systems (Strubell et al., 2019).

1.4. Exploring the need for energy-efficient AI algorithms and hardware

As the demand for AI continues to grow, there is a pressing need to develop energy-efficient algorithms and hardware to mitigate the environmental impact of AI computations. The energy consumption of AI systems is a significant concern, considering the carbon emissions associated with non-renewable energy sources (Rolnick et al., 2022).

Researchers are actively exploring techniques to improve the energy efficiency of AI algorithms. Model compression, for instance, aims to reduce the computational requirements of deep neural networks by pruning unnecessary connections or reducing the precision of weights and activations (Han et al., 2015). This approach can significantly decrease the energy consumption and inference time without sacrificing model performance.

Another approach is quantisation, which involves representing numerical values with fewer bits. By reducing the precision of parameters and activations, quantisation reduces memory usage and computational complexity, leading to energy savings during both training and inference (Hubara et al., 2016). Efforts are also being made to improve the energy efficiency of training algorithms. Gradient compression techniques, such as sparsification and quantisation, aim to reduce the communication overhead between distributed devices during distributed training, thus decreasing the energy consumption (Alistarh et al., 2017). Additionally, advancements in optimisation algorithms and learning rate schedules can minimise the number of training iterations required, resulting in energy savings (You et al., 2017).

The development of energy-efficient AI hardware is also a crucial aspect of mitigating energy consumption. Traditional computing architectures are often not optimised for AI workloads, leading to inefficient energy usage. To address this, researchers are exploring new hardware designs, including neuromorphic computing and memristive devices, which mimic the structure and functioning of the human brain, offering potential energy efficiency improvements (Merolla et al., 2014; Prezioso et al., 2015).

---

[8] European Commission. (n.d.). EU Climate Action. https://clck.ru/36kxSS

2. Electronic Waste Generation

In addition to the energy-intensive nature of AI computations, the hardware used in AI systems also contributes to another significant environmental challenge: electronic waste generation. The rapid pace of technological advancement and the constant need for more powerful hardware result in a high turnover rate, leading to a growing accumulation of electronic waste (Ferro et al., 2021).

AI hardware, including GPUs, application-specific integrated circuits (ASICs), and other specialised components, have relatively short lifespans due to the relentless progress in technology. As newer generations of hardware are developed, older ones quickly become obsolete and are often discarded, exacerbating the issue of electronic waste[9].

The disposal of AI hardware contributes to the release of hazardous substances and materials into the environment when not properly managed. These substances can contaminate soil, water, and air, posing risks to human health and ecosystems. The improper disposal of electronic waste not only leads to environmental degradation but also wastes valuable resources embedded in the hardware. Moreover, the disposal of hardware that contains toxic materials such as lead, mercury, and flame retardants can further contribute to pollution if not handled properly[10].

To tackle the issue of electronic waste generation in the AI industry, it is crucial to implement sustainable practices. One approach is to promote the reuse and recycling of AI hardware. By refurbishing and remanufacturing older hardware, its lifespan can be extended, reducing the need for constant production of new devices (Ferro et al., 2021). Additionally, implementing take-back programs and establishing recycling facilities ensure that discarded hardware is properly managed and valuable materials are recovered for reuse[11].

In the design and manufacturing of AI hardware, eco-friendly principles should be embraced. Using materials with lower environmental impacts, designing for recyclability, and reducing the presence of hazardous substances can contribute to a more sustainable hardware lifecycle. Adopting modular designs that allow for component replacement and upgrading can also help prolong the usefulness of AI hardware, reducing the frequency of complete device replacement (Ferro et al., 2021).

---

9 Baldé, C. P., Forti, V., Gray, V., Kuehr, R., & Stegmann, P. (2017). The global e-waste monitor 2017: Quantities, flows and resources. United Nations University, International Telecommunication Union, and International Solid Waste Association.

10 Ibid.

11 Ibid.

2.1. The rapid pace of AI hardware advancements

The hardware technologies in the field of AI are undergoing rapid advancements, fueled by continuous innovation that leads to the creation of increasingly powerful and efficient AI systems (Amodei et al., 2016). A notable development in AI hardware is the evolution of GPUs into a key component for AI computations. Originally designed for graphics rendering, GPUs have found extensive adoption in AI due to their ability to handle parallel processing tasks effectively (Amodei et al., 2016). Their high throughput and computational power make them well-suited for training and running AI models.

Furthermore, specialised hardware known as ASICs has emerged to cater specifically to AI workloads. ASICs offer improved performance and energy efficiency by customising the hardware architecture to optimise AI algorithm execution (Amodei et al., 2016). These dedicated AI chips provide higher computational density and faster processing speeds compared to general-purpose processors.

The rapid advancements in AI hardware have been instrumental in enabling significant breakthroughs across various AI applications. In computer vision, for example, the availability of high-performance hardware has facilitated complex image recognition and object detection tasks with remarkable accuracy (Amodei et al., 2016). Similarly, in natural language processing, powerful hardware accelerates the training and inference of language models, enabling applications such as machine translation and sentiment analysis.

However, the swift progress in AI hardware also brings challenges. The rapid turnover of hardware due to newer generations becoming available leads to a significant accumulation of electronic waste. Outdated hardware components contribute to the growing e-waste problem, requiring proper disposal and recycling measures to minimise environmental impact (Ferro et al., 2021).

The continuous introduction of new AI hardware also presents a learning curve for developers and researchers. Staying up to date with the latest hardware technologies demands constant adaptation, training, and investment, posing challenges for those involved in AI development (Amodei et al., 2016). Furthermore, optimising AI algorithms and software to leverage the capabilities of different hardware architectures adds complexity to the development process.

2.2. Device lifecycles and the E-waste predicament

The rapid advancement of AI technologies has led to a proliferation of electronic devices, resulting in a concerning rise in electronic waste, or e-waste, which poses significant environmental and health risks[12]. The lifecycles of AI hardware play a crucial role in determining the extent of e-waste generated and the environmental impact associated with it.

[12] Ibid.

The lifecycle of AI hardware begins with the extraction of raw materials and the manufacturing process. The production of AI devices involves the extraction of precious metals, rare earth elements, and other valuable materials, many of which are non-renewable and require substantial energy inputs (Ferro et al., 2021). The extraction and processing of these materials contribute to environmental degradation and often involve hazardous substances that can harm ecosystems and human health.

As AI hardware advances rapidly, the lifecycle of devices becomes shorter, with newer models frequently replacing older ones. This phenomenon, known as planned obsolescence, exacerbates the e-waste predicament, as outdated AI devices are discarded, leading to a significant accumulation of electronic waste[13]. E-waste contains hazardous components such as lead, mercury, and flame retardants, which can leach into the environment and contaminate soil, water sources, and air if not properly managed.

The improper disposal and inadequate recycling of e-waste further compound the problem. Many electronic devices end up in landfills or are incinerated, releasing toxic substances and contributing to air and soil pollution[14]. Inadequate recycling practices also result in the loss of valuable resources that could be recovered and reused.

Policymakers play a crucial role in establishing regulations and incentives to promote proper e-waste management. Policies such as extended producer responsibility (EPR) can hold manufacturers accountable for the environmental impact of their products throughout their lifecycle, encouraging them to adopt sustainable practices and invest in recycling infrastructure[15]. Additionally, the development of effective collection systems, recycling programmes, and refurbishment initiatives can help divert AI devices from landfills and promote their reuse.

The circular economy approach offers a promising solution to the e-waste predicament. It emphasises the reuse, refurbishment, and recycling of electronic devices, aiming to minimise resource consumption and environmental impact (Ferro et al., 2021). By adopting circular economy principles, AI hardware can be designed and managed in a way that maximises its lifespan and reduces the need for constant upgrades, thus mitigating the generation of e-waste.

2.3. Strategies for responsible e-waste management in AI

In order to address the environmental concerns associated with electronic waste generated by AI hardware, several strategies have been proposed to promote responsible e-waste

13 Baldé, C. P., Forti, V., Gray, V., Kuehr, R., & Stegmann, P. (2017). The global e-waste monitor 2017: Quantities, flows and resources. United Nations University, International Telecommunication Union, and International Solid Waste Association.

14 Ibid.

15 Ibid.

management throughout the AI lifecycle. These strategies aim to mitigate the adverse impacts of e-waste disposal and contribute to a more sustainable approach to AI technology.

1. Incorporating Design for Disassembly (DfD) and Design for Recycling (DfR) principles in the design and manufacturing of AI hardware can facilitate the efficient separation and recycling of components. By ensuring that devices are designed with ease of disassembly and recyclability in mind, the amount of e-waste generated can be reduced.

2. The concept of Extended Producer Responsibility holds manufacturers accountable for the entire lifecycle of their products, including their proper disposal (Kahhat et al., 2008). Implementing EPR regulations specific to AI hardware can incentivize manufacturers to design products with recyclability in mind and take responsibility for their environmentally sound disposal and recycling.

3. Establishing effective take-back and recycling programs is crucial for facilitating the responsible disposal of AI hardware. Manufacturers can collaborate with specialised e-waste recyclers or set up collection points to ensure the proper recycling of AI devices and prevent them from ending up in landfills or informal recycling facilities.

Embracing the principles of a circular economy can help minimise e-waste generation by promoting resource efficiency and product reuse (Geissdoerfer et al., 2017). Strategies such as refurbishing and repurposing AI hardware, as well as creating secondary markets for used devices, can extend the lifespan of AI systems and reduce the need for new production.

Continued research and development of advanced recycling technologies are essential for improving the efficiency and effectiveness of e-waste recycling (Widmer et al., 2005). Innovations such as hydrometallurgical and biotechnological processes can extract valuable materials from AI hardware while minimising environmental impact and reducing the reliance on traditional extraction methods.

By implementing these strategies, responsible e-waste management practices can be integrated into the AI industry, leading to a more sustainable approach to AI hardware production, use, and disposal.

3. Data Centre Infrastructure

Data centres have witnessed significant growth in recent years due to the increasing demand for digital services. This expansion has resulted in a heightened environmental impact. The construction and operation of data centres require substantial land and resources, contributing to land use changes and habitat destruction (Mell & Grance, 2011). Moreover, the proliferation of data centres in urban areas has raised concerns about their impact on local communities and infrastructure.

Data centres are renowned for their high energy consumption. The constant operation of servers, networking equipment, and cooling systems demands a considerable amount of electricity. Cooling data centres poses particular challenges. The heat generated by servers and other IT equipment needs efficient dissipation to maintain optimal operating conditions. However, traditional cooling methods, such as air conditioning, are energy-intensive and inefficient. This has prompted the exploration of innovative cooling technologies, including liquid cooling and advanced airflow management systems, to enhance energy efficiency and reduce the environmental impact of data centres (Masanet et al., 2020).

Water is a vital resource used in data centres for cooling purposes. However, the substantial water consumption of data centres can strain local water resources, especially in regions already grappling with water scarcity or competing demands. Cooling towers, relying on evaporation, can consume significant volumes of water.

To address the environmental impact of data centres, industry stakeholders are actively exploring and implementing sustainable practices. These practices include:

Energy-efficient design: Data centres can adopt energy-efficient design principles, such as optimising server utilisation, improving power distribution systems, and utilising energy-efficient hardware. These measures can significantly reduce energy consumption and carbon emissions (Beloglazov et al., 2011).

Transitioning to renewable energy sources, such as solar or wind power, can assist data centres in reducing their dependence on fossil fuels and decreasing greenhouse gas emissions.

Rather than dissipating the heat generated by data centres, waste heat can be captured and utilised for other purposes, such as heating buildings or generating electricity. This approach maximises the energy efficiency of data centres and reduces their overall environmental impact.

Implementing water-efficient cooling technologies, such as closed-loop cooling systems and water-saving cooling towers, can help reduce water consumption in data centres. Additionally, recycling and reusing water within data centre operations can minimise the strain on local water resources.

By adopting these sustainable practices, data centres can strike a balance between meeting the increasing demand for digital services and minimising their environmental impact, contributing to a more sustainable and responsible digital infrastructure.

4. Understanding biases in AI training data

AI algorithms heavily rely on training data to make informed decisions. However, these datasets can often contain inherent biases, which can lead to biased outcomes in environmental decision-making. Biases in training data can arise from various sources,

including historical data reflecting existing societal inequalities and systemic biases (Caliskan et al., 2017). It is crucial to recognise and address these biases to ensure fair and equitable environmental decision-making processes.

Biased AI applications in environmental decision-making can exacerbate existing environmental disparities faced by marginalised communities. For example, if AI algorithms are trained on datasets that disproportionately represent affluent areas, decisions regarding resource allocation or environmental policies may neglect the needs and concerns of marginalised communities (Benjamin, 2019). This further marginalises these communities, perpetuating environmental injustices.

Biased AI applications can perpetuate and amplify inequalities by reinforcing existing social, economic, and environmental disparities. For instance, if AI algorithms are biased against certain demographics or geographic areas, it can lead to unequal distribution of environmental benefits, such as access to clean air, water, or green spaces. Furthermore, biased algorithms can result in discriminatory outcomes, such as disproportionate pollution burdens or inadequate environmental protections in marginalised communities.

To mitigate the biases and promote fairness in AI environmental decision-making, several measures need to be taken:

It is essential to ensure that AI training datasets encompass diverse perspectives and accurately represent the affected communities. This requires careful curation of data to address underrepresentation and avoid reinforcing existing biases (Sweeney, 2013).

Developing AI algorithms that are transparent and explainable allows for scrutiny and identification of biases. This helps stakeholders, including affected communities, to understand how decisions are made and challenge potential biases (Burrell, 2016).

Continual monitoring and evaluation of AI systems are crucial to identify and rectify biases that may emerge over time. This involves ongoing assessment of AI applications' impacts on different populations and their alignment with equity and fairness goals (Crawford & Calo, 2016).

Involving affected communities in the design, implementation, and evaluation of AI environmental decision-making processes can help ensure fairness and equity.

By addressing biases in AI training data, acknowledging environmental disparities faced by marginalised communities, and implementing measures to promote fairness and equity, it is possible to mitigate the risks of AI amplifying environmental injustices. Responsible and inclusive AI applications can support informed and equitable decision-making processes that contribute to a more just and sustainable environment for all.

5. Disruption of Natural Ecosystems

The expansion of AI technologies and their integration into various sectors has raised concerns about their potential impact on natural ecosystems. One area of concern is the disruption of wildlife habitats and migration patterns. AI-driven infrastructure, such as the construction of data centers and communication networks, often requires significant land use, leading to habitat fragmentation and loss. This disruption can have adverse effects on wildlife populations by limiting their access to resources and disrupting crucial migration routes, ultimately posing a threat to biodiversity and ecological resilience.

The use of AI for environmental monitoring and conservation presents both opportunities and challenges. On one hand, AI enables efficient data collection, analysis, and interpretation, thereby enhancing our understanding of biodiversity, climate change, and ecosystem health. It enables us to detect patterns, make predictions, and inform conservation strategies. On the other hand, an overreliance on AI may result in a reduction in field-based research and human involvement, potentially overlooking the nuanced ecological processes that can only be observed through direct observation (Koh & Wich, 2012).

To mitigate the ecological disruption caused by AI, it is crucial to adopt responsible deployment practices. This includes conducting comprehensive environmental impact assessments before implementing AI technologies, evaluating potential risks to ecosystems, and identifying appropriate mitigation strategies. Moreover, it is important to integrate AI into existing conservation strategies and involve local communities in decision-making processes. This participatory approach fosters a holistic understanding of ecological systems and facilitates the co-design of AI applications that benefit both biodiversity and human well-being.

6. Existing Regulations Related to AI's Environmental Impact in the European Union

The growth of artificial intelligence has prompted governments and regulatory bodies to address its potential environmental impact. Some countries and regions have already taken steps to regulate the ecological cost of AI.

In the European Union, the EcoDesign Directive (2009/125/EC) has been extended to cover servers and data storage products since March 2020. This regulation sets minimum energy efficiency requirements for these products, including those used in AI hardware. It aims to reduce energy consumption and curb the environmental impact of data centers and other AI infrastructure components[16].

[16] Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products (recast) (Text with EEA relevance). (2009). Official Journal of the European Union, L 285, 10–35. https://clck.ru/36kxU5

Along with the EcoDesign Directive, the Waste Electrical and Electronic Equipment (WEEE) Directive plays a crucial role in the sustainable management of electronic waste, including AI hardware components. The WEEE Directive outlines rules for the proper handling and disposal of electronic waste, ensuring that discarded AI hardware is managed in an environmentally responsible manner. The responsibility for the collection and recycling of e-waste is placed on manufacturers and users, promoting the circular economy and minimizing the environmental impact of AI hardware disposal[17].

As part of the WEEE Directive's evaluation process, a public consultation on the EU Directive on waste electrical and electronic equipment was scheduled for June 2023. This consultation allows stakeholders and the public to provide feedback and input on the effectiveness and future improvements of the WEEE Directive.

The European Union has also implemented the Regulation (EU) 2019/424 on the eco-design requirements for servers and data storage products. This regulation, which entered into force in March 2020, aims to set minimum energy efficiency requirements for these products, including those used in AI hardware, with the purpose of reducing energy consumption and curbing the environmental impact of data centers and other AI infrastructure components[18].

These regulations within the European Union demonstrate the commitment to address the environmental impact of artificial intelligence and promote sustainable practices in the technology sector. By setting energy efficiency standards and promoting responsible e-waste management, the EU aims to foster a greener and more environmentally friendly approach to AI development and deployment.

Conclusion

In conclusion, when reflecting on the hidden ecological cost of AI, it becomes evident that we must acknowledge and address the environmental implications that come with its development and integration. The energy-intensive nature of AI computations, the generation of electronic waste, the disruption of natural ecosystems, and the potential for biased decision-making all highlight the need for proactive measures. By recognising the importance of sustainable practices such as energy-efficient algorithms, transitioning to renewable energy sources, responsible e-waste management, and ethical considerations, we can strive towards a more harmonious and environmentally conscious integration of AI.

---

17 Consolidated text: Directive 2012/19/EU of the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment (WEEE) (recast) (Text with EEA relevance). https://clck.ru/36kxYS

18 Commission Regulation (EU) 2019/424 of 15 March 2019 laying down ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) No 617/2013 (Text with EEA relevance). (2019). Official Journal of the European Union, L 74, 46–66. https://clck.ru/36kxbm

It is our collective responsibility to navigate the path towards a better future where AI benefits both humanity and the planet. By prioritising environmental sustainability and taking proactive steps to mitigate the ecological footprint of AI, we can create a future that harnesses its potential while preserving and protecting our natural resources. Through collaboration, research, and the development of policies and regulations, we can shape the evolution of AI towards a more sustainable and ethically sound direction.

References

Alistarh, D., Grubic, D., Li, J., Tomioka, R., & Vojnovic, M. (2017). QSGD: Communication-efficient SGD via gradient quantization and encoding. *Advances in neural information processing systems*, *30*. https://doi.org/10.48550/arXiv.1610.02132

Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., & Mané, D. (2016). *Concrete problems in AI safety*. https://doi.org/10.48550/arXiv.1606.06565

Beloglazov, A., Buyya, R., Lee, Y. C., & Zomaya, A. (2011). A taxonomy and survey of energy-efficient data centers and cloud computing systems. *Advances in computers*, *82*, 47–111. https://doi.org/10.1016/B978-0-12-385512-1.00003-7

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim code*. Cambridge: Polity.

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1). https://doi.org/10.1177/2053951715622512

Caliskan, A., Bryson, J. J., & Narayanan, A. (2017). Semantics derived automatically from language corpora contain human-like biases. *Science*, *356*(6334), 183–186. https://doi.org/10.1126/science.aal4230

Crawford, K., & Calo, R. (2016). There is a blind spot in AI research. *Nature*, *538*(7625), 311–313. https://doi.org/10.1038/538311a

Dhar, P. (2020). The carbon impact of artificial intelligence. *Nat. Mach. Intell.*, *2*(8), 423–425. https://doi.org/10.1038/s42256-020-0219-9

Ding, Q., Zhu, R., Liu, H., & Ma, M. (2021). An overview of machine learning-based energy-efficient routing algorithms in wireless sensor networks. *Electronics*, *10*(13), 1539. https://doi.org/10.3390/electronics10131539

Ferro, M., Silva, G. D., de Paula, F. B., Vieira, V., & Schulze, B. (2021). Towards a sustainable artificial intelligence: A case study of energy efficiency in decision tree algorithms. *Concurrency and Computation: Practice and Experience*, *e6815*. https://doi.org/10.1002/cpe.6815

Geissdoerfer, M., Savaget, P., Bocken, N. M., & Hultink, E. J. (2017). The Circular Economy–A new sustainability paradigm? *Journal of cleaner production*, *143*, 757–768. https://doi.org/10.1016/j.jclepro.2016.12.048

Han, S., Pool, J., Tran, J., & Dally, W. (2015). Learning both weights and connections for efficient neural network. In *Advances in neural information processing systems 28*. https://doi.org/10.48550/arXiv.1506.02626

Hanus, N., Newkirk, A., & Stratton, H. (2023). Organizational and psychological measures for data center energy efficiency: barriers and mitigation strategies. *Energy Efficiency*, *16*(1), 1–18. https://doi.org/10.1007/s12053-022-10078-1

Henderson, P., Islam, R., Bachman, P., Pineau, J., Precup, D., & Meger, D. (2018). Deep reinforcement learning that matters. In *Proceedings of the AAAI conference on artificial intelligence* (Vol. 32, No. 1). https://doi.org/10.1609/aaai.v32i1.11694

Hubara, I., Courbariaux, M., Soudry, D., El-Yaniv, R., & Bengio, Y. (2016). Quantized neural networks: Training neural networks with low precision weights and activations. *The Journal of Machine Learning Research*, *18*(1), 6869–6898. https://doi.org/10.48550/arXiv.1609.07061

Kahhat, R., Kim, J., Xu, M., Allenby, B., Williams, E., & Zhang, P. (2008). Exploring e-waste management systems in the United States. *Resources, conservation and recycling*, *52*(7), 955–964. https://doi.org/10.1016/j.resconrec.2008.03.002

Koh, L. P., & Wich, S. A. (2012). Dawn of drone ecology: low-cost autonomous aerial vehicles for conservation. *Tropical conservation science*, *5*(2), 121–132. https://doi.org/10.1177/194008291200500202

Masanet, E., Shehabi, A., Lei, N., Smith, S., & Koomey, J. (2020). Recalibrating global data center energy-use estimates. *Science*, *367*(6481), 984–986. https://doi.org/10.1126/science.aba3758

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. Special Publication (NIST SP). National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-145

Merolla, P. A., Arthur, J. V., Alvarez-Icaza, R., Cassidy, A. S., Sawada, J., Akopyan, F., ... & Modha, D. S. (2014). A million spiking-neuron integrated circuit with a scalable communication network and interface. *Science*, *345*(6197), 668–673. https://doi.org/10.1126/science.1254642

Prezioso, M., Merrikh-Bayat, F., Hoskins, B. D., Adam, G. C., Likharev, K. K., & Strukov, D. B. (2015). Training and operation of an integrated neuromorphic network based on metal-oxide memristors. *Nature*, *521*(7550), 61–64. https://doi.org/10.1038/nature14441

Ram, M., Child, M., Aghahosseini, A., Bogdanov, D., Lohrmann, A., & Breyer, C. (2018). A comparative analysis of electricity generation costs from renewable, fossil fuel and nuclear sources in G20 countries for the period 2015-2030. *Journal of Cleaner Production*, *199*, 687–704. https://doi.org/10.1016/j.jclepro.2018.07.159

Rolnick, D., Donti, P. L., Kaack, L. H., Kochanski, K., Lacoste, A., Sankaran, K., ... & Bengio, Y. (2022). Tackling climate change with machine learning. *ACM Computing Surveys (CSUR)*, *55*(2), 1–96. https://doi.org/10.1145/3485128

Schwartz, R., Dodge, J., Smith, N. A., & Etzioni, O. (2020). Green AI. *Communications of the ACM*, *63*(12), 54–63. https://doi.org/10.1145/3381831

Şerban, A. C., & Lytras, M. D. (2020). Artificial intelligence for smart renewable energy sector in Europe – smart energy infrastructures for next generation smart cities. *IEEE access*, *8*, 77364–77377. https://doi.org/10.1109/ACCESS.2020.2990123

Shah, A., Bash, C., Sharma, R., Christian, T., Watson, B. J., & Patel, C. (2010). The environmental footprint of data centers. In *ASME 2009 InterPACK Conference* (Vol. 2, pp. 653–662). San Francisco, CA. https://doi.org/10.1115/InterPACK2009-89036

Strubell, E., Ganesh, A., & McCallum, A. (2019). Energy and policy considerations for deep learning in NLP. https://doi.org/10.48550/arXiv.1906.02243

Sweeney, L. (2013). Discrimination in online ad delivery. *Communications of the ACM*, *56*(5), 44–54. https://doi.org/10.1145/2447976.2447990

Widmer, R., Oswald-Krapf, H., Sinha-Khetriwal, D., Schnellmann, M., & Böni, H. (2005). Global perspectives on e-waste. *Environmental Impact Assessment Review*, *25*(5), 436–458. https://doi.org/10.1016/j.eiar.2005.04.001

You, Y., Gitman, I., & Ginsburg, B. (2017). *Large batch training of convolutional networks*. https://doi.org/10.48550/arXiv.1708.03888

Author information

Alesia Zhuk – PhD Candidate, Law and Philosophy Group at Universitat Pompeu Fabra, Teaching Assistant, Institut Barcelona d'Estudis Internacionals
Address: Ramon Trias Fargas, 25-27. 08005 Barcelona, Spain
E-mail: alesia.zhuk@ug.uchile.cl
ORCID ID: https://orcid.org/0000-0002-6295-6839
Google Scholar ID: https://scholar.google.com/citations?user=PVCH_B0AAAAJ

Conflicts of interest

The authors declare no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 29, 2023
Date of approval – August 21, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:364.25:504.75:004.8
EDN: https://elibrary.ru/ffvrya
DOI: https://doi.org/10.21202/jdtl.2023.40

Воздействие искусственного интеллекта на окружающую среду: скрытые экологические издержки и этико-правовые вопросы

Алеся Жук

Университет Помпеу Фабра
г. Барселона, Испания

Ключевые слова

алгоритмическая предвзятость,
искусственный интеллект,
потребление энергии,
право,
природные экосистемы,
устойчивое развитие,
центр обработки данных,
цифровые технологии,
экологические издержки,
электронные отходы

Аннотация

Цель: выявление скрытых экологических издержек, связанных с разработкой, внедрением и развитием технологий искусственного интеллекта, с целью его устойчивой и гармоничной интеграции с различными секторами экономики путем определения оптимальных нравственно-этических и политико-правовых стратегий.

Методы: в основе проведенного исследования лежит экологический подход к разработке и внедрению искусственного интеллекта, междисциплинарный и политико-правовой анализ экологических проблем и рисков алгоритмической предвзятости, ошибок в алгоритмах искусственного интеллекта и процессах принятия решений, которые могут усугубить экологическое неравенство и несправедливость в отношении к окружающей среде. Кроме того, подвержены анализу вызванные развитием технологий искусственного интеллекта последствия разрушений природных экосистем, обусловленные энергоемким характером связанных с ним вычислений, растущим влиянием центров обработки данных на потребление энергии и проблем с их охлаждением, образование электронных отходов из-за быстрого совершенствования оборудования и др.

Результаты: проведенный анализ показывает разнообразие экологических, этических и политико-правовых проблем, связанных с обучением, использованием и развитием искусственного интеллекта, потребляющего значительное количество энергии (в основном из невозобновляемых источников), что приводит к увеличению выбросов углерода и создает препятствия для дальнейшего устойчивого экологического развития. Неправильная утилизация оборудования искусственного интеллекта усугубляет проблему электронных отходов, загрязнения планеты, еще больше нанося ущерб окружающей среде. Ошибки в алгоритмах искусственного интеллекта и процессах

принятия решений ведут к несправедливости в отношении окружающей среды и экологическому неравенству. Технологии искусственного интеллекта могут нарушать природные экосистемы, ставя под угрозу среду обитания диких животных и модели миграции.

Научная новизна: исследование экологических последствий использования и дальнейшего развития искусственного интеллекта, вызванных в связи с этим экологических нарушений и издержек устойчивого развития позволяет определить научный поиск оптимальных стратегий минимизации вреда окружающей среде, в котором правоведам и юристам предстоит установить этико-правовые и политико-правовые решения на национальном и наднациональном уровнях.

Практическая значимость: понимание экологического воздействия искусственного интеллекта имеет решающее значение для политиков, юристов, исследователей, отраслевых специалистов при разработке стратегий минимизации вреда окружающей среде. Полученные данные подчеркивают важность реализации энергоэффективных алгоритмов, перехода на возобновляемые источники энергии, внедрения ответственной практики обращения с электронными отходами, обеспечения справедливости при принятии решений искусственным интеллектом и учета этических соображений и правил его внедрения.

Для цитирования

Жук, А. (2023). Воздействие искусственного интеллекта на окружающую среду: скрытые экологические издержки и этико-правовые вопросы. *Journal of Digital Technologies and Law*, *1*(4), 932–954. https://doi.org/10.21202/jdtl.2023.40

Список литературы

Alistarh, D., Grubic, D., Li, J., Tomioka, R., & Vojnovic, M. (2017). QSGD: Communication-efficient SGD via gradient quantization and encoding. *Advances in neural information processing systems*, *30*. https://doi.org/10.48550/arXiv.1610.02132

Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., & Mané, D. (2016). *Concrete problems in AI safety*. https://doi.org/10.48550/arXiv.1606.06565

Beloglazov, A., Buyya, R., Lee, Y. C., & Zomaya, A. (2011). A taxonomy and survey of energy-efficient data centers and cloud computing systems. *Advances in computers*, *82*, 47–111. https://doi.org/10.1016/B978-0-12-385512-1.00003-7

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim code*. Cambridge: Polity.

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1). https://doi.org/10.1177/2053951715622512

Caliskan, A., Bryson, J. J., & Narayanan, A. (2017). Semantics derived automatically from language corpora contain human-like biases. *Science*, *356*(6334), 183–186. https://doi.org/10.1126/science.aal4230

Crawford, K., & Calo, R. (2016). There is a blind spot in AI research. *Nature*, *538*(7625), 311–313. https://doi.org/10.1038/538311a

Dhar, P. (2020). The carbon impact of artificial intelligence. *Nat. Mach. Intell.*, *2*(8), 423–425. https://doi.org/10.1038/s42256-020-0219-9

Ding, Q., Zhu, R., Liu, H., & Ma, M. (2021). An overview of machine learning-based energy-efficient routing algorithms in wireless sensor networks. *Electronics*, *10*(13), 1539. https://doi.org/10.3390/electronics10131539

Ferro, M., Silva, G. D., de Paula, F. B., Vieira, V., & Schulze, B. (2021). Towards a sustainable artificial intelligence: A case study of energy efficiency in decision tree algorithms. *Concurrency and Computation: Practice and Experience*, *e6815*. https://doi.org/10.1002/cpe.6815

Geissdoerfer, M., Savaget, P., Bocken, N. M., & Hultink, E. J. (2017). The Circular Economy–A new sustainability paradigm? *Journal of cleaner production*, *143*, 757–768. https://doi.org/10.1016/j.jclepro.2016.12.048

Han, S., Pool, J., Tran, J., & Dally, W. (2015). Learning both weights and connections for efficient neural network. In *Advances in neural information processing systems 28*. https://doi.org/10.48550/arXiv.1506.02626

Hanus, N., Newkirk, A., & Stratton, H. (2023). Organizational and psychological measures for data center energy efficiency: barriers and mitigation strategies. *Energy Efficiency*, *16*(1), 1–18. https://doi.org/10.1007/s12053-022-10078-1

Henderson, P., Islam, R., Bachman, P., Pineau, J., Precup, D., & Meger, D. (2018). Deep reinforcement learning that matters. In *Proceedings of the AAAI conference on artificial intelligence* (Vol. 32, No. 1). https://doi.org/10.1609/aaai.v32i1.11694

Hubara, I., Courbariaux, M., Soudry, D., El-Yaniv, R., & Bengio, Y. (2016). Quantized neural networks: Training neural networks with low precision weights and activations. *The Journal of Machine Learning Research*, *18*(1), 6869–6898. https://doi.org/10.48550/arXiv.1609.07061

Kahhat, R., Kim, J., Xu, M., Allenby, B., Williams, E., & Zhang, P. (2008). Exploring e-waste management systems in the United States. *Resources, conservation and recycling*, *52*(7), 955–964. https://doi.org/10.1016/j.resconrec.2008.03.002

Koh, L. P., & Wich, S. A. (2012). Dawn of drone ecology: low-cost autonomous aerial vehicles for conservation. *Tropical conservation science*, *5*(2), 121–132. https://doi.org/10.1177/194008291200500202

Masanet, E., Shehabi, A., Lei, N., Smith, S., & Koomey, J. (2020). Recalibrating global data center energy-use estimates. *Science*, *367*(6481), 984–986. https://doi.org/10.1126/science.aba3758

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. Special Publication (NIST SP). National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-145

Merolla, P. A., Arthur, J. V., Alvarez-Icaza, R., Cassidy, A. S., Sawada, J., Akopyan, F., ... & Modha, D. S. (2014). A million spiking-neuron integrated circuit with a scalable communication network and interface. *Science*, *345*(6197), 668–673. https://doi.org/10.1126/science.1254642

Prezioso, M., Merrikh-Bayat, F., Hoskins, B. D., Adam, G. C., Likharev, K. K., & Strukov, D. B. (2015). Training and operation of an integrated neuromorphic network based on metal-oxide memristors. *Nature*, *521*(7550), 61–64. https://doi.org/10.1038/nature14441

Ram, M., Child, M., Aghahosseini, A., Bogdanov, D., Lohrmann, A., & Breyer, C. (2018). A comparative analysis of electricity generation costs from renewable, fossil fuel and nuclear sources in G20 countries for the period 2015-2030. *Journal of Cleaner Production*, *199*, 687–704. https://doi.org/10.1016/j.jclepro.2018.07.159

Rolnick, D., Donti, P. L., Kaack, L. H., Kochanski, K., Lacoste, A., Sankaran, K., ... & Bengio, Y. (2022). Tackling climate change with machine learning. *ACM Computing Surveys (CSUR)*, *55*(2), 1–96. https://doi.org/10.1145/3485128

Schwartz, R., Dodge, J., Smith, N. A., & Etzioni, O. (2020). Green AI. *Communications of the ACM*, *63*(12), 54–63. https://doi.org/10.1145/3381831

Şerban, A. C., & Lytras, M. D. (2020). Artificial intelligence for smart renewable energy sector in Europe – smart energy infrastructures for next generation smart cities. *IEEE access*, *8*, 77364–77377. https://doi.org/10.1109/ACCESS.2020.2990123

Shah, A., Bash, C., Sharma, R., Christian, T., Watson, B. J., & Patel, C. (2010). The environmental footprint of data centers. In *ASME 2009 InterPACK Conference* (Vol. 2, pp. 653–662). San Francisco, CA. https://doi.org/10.1115/InterPACK2009-89036

Strubell, E., Ganesh, A., & McCallum, A. (2019). Energy and policy considerations for deep learning in NLP. https://doi.org/10.48550/arXiv.1906.02243

Sweeney, L. (2013). Discrimination in online ad delivery. *Communications of the ACM*, *56*(5), 44–54. https://doi.org/10.1145/2447976.2447990

Widmer, R., Oswald-Krapf, H., Sinha-Khetriwal, D., Schnellmann, M., & Böni, H. (2005). Global perspectives on e-waste. *Environmental Impact Assessment Review*, *25*(5), 436–458. https://doi.org/10.1016/j.eiar.2005.04.001

You, Y., Gitman, I., & Ginsburg, B. (2017). *Large batch training of convolutional networks*. https://doi.org/10.48550/arXiv.1708.03888

Сведения об авторе

Алеся Жук – соискатель степени PhD, факультет права и философии, Университет Помпеу Фабра; ассистент преподавателя, Барселонский институт международных исследований
Адрес: 08005, Испания, Барселона, Рамон Триас Фаргас, 25-27
E-mail: alesia.zhuk@ug.uchile.cl
ORCID ID: https://orcid.org/0000-0002-6295-6839
Google Scholar ID: https://scholar.google.com/citations?user=PVCH_B0AAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.53.91 / Экологическое право в отдельных странах
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 29 июня 2023 г.
Дата одобрения после рецензирования – 21 августа 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.41

Ethics of Artificial Intelligence and Robotics: Key Issues and Modern Ways to Solve Them

Nidhika Yadav

Independent Researcher
New Delhi, India

Keywords

artificial intelligence,
ChatGPT,
cyber security,
data privacy,
digital technologies,
ethics,
law,
robot,
robotics,
safety

Abstract

Objective: modern achievements in the development and dissemination of digital technologies have attracted the attention of scholars and practitioners to the discussion of key ethical issues related to artificial intelligence and robotics. Hence, this study presents the most relevant of these issues, posing new challenges for legal scholars and practitioners to develop the regulation of artificial intelligence and robotics in terms of technology moralization.

Methods: the research used practice- and risk-oriented approaches, complemented by multidisciplinary analysis of documents (European principles and codes of ethics) and studies, including those devoted to various problems of artificial intelligence and robotics.

Results: the article identifies key ethical issues in the field of artificial intelligence and robotics. It is established that the key ethical issues involved can be solved if they are legally formalized and implemented at the international level. The algorithm proposed by the author, based on the analysis of the digital technologies application, will allow improving the moral actions of technologies in the process of their decision making.

Scientific novelty: the article presents the latest ethical problems that concern scientists and practitioners in the field of artificial intelligence and robotics, and the methods of their solution by ethical and legal means aimed at moralizing technology and increasing its responsibility.

Practical significance: all solutions presented in the article have practical significance and are ready for wide implementation at the international level. Their formalization in normative form and subsequent compliance will reduce the harm that artificial intelligence may cause in applied fields, including robotics using artificial intelligence. Regulatory, including legislative, decisions must therefore be taken as soon as possible to ensure that artificial intelligence and robotics become reliable tools for these systems to be used at work, at home, and in other areas such as shopping centers, stores, schools, universities, etc.

For citation

Yadav, N. (2023). Ethics of artificial intelligence and robotics: key issues and modern ways to solve them. *Journal of Digital Technologies and Law, 1*(4), 955–972. https://doi.org/10.21202/jdtl.2023.41

Content

Introduction

Artificial Intelligence (AI) (Rich et al., 2009) has gained a lot of momentum all of its own recently. The progress in AI was immense in the past few years. The progress is record-breaking in each of its application areas (Saveliev et al., 2021). Further, many segments of recent developments in AI were, firstly, never thought of and, secondly, many things were never imagined as well (Xiao-Fan et al., 2023; Kumar et al., 2023). ChatGPT is one such

example wherein even the makers of this AI product were stunned in surprise by the peaks of development they made. ChatGPT is just one such example; the progress is seen in many domains, not just in generative texts, but in many parts of AI research. Some of these are discussed in this paper.

Artificial Intelligence (AI) is a term coined for a branch of science that deals with mimicking the working of the human brain to accomplish difficult work that humans perform. The aim was to ease human work and perform like humans or to provide auxiliary help in tasks presented to humans. The subject AI (Rich et al., 2009; Stahl, 2021; Mueller, 2012) is constituted of an amalgamation of many fields such as computer science, mathematics, cognitive sciences, and psychology to mention a few. The inception of AI was in the early 50's and it gained the interest of researchers since then (Turing, 2009; Schank, 1991). The subject was developed to build algorithms and/or machines that can do work or perform like humans and in some cases where humans could not do work, AI-based intelligent machines could do work for humans, for example, mining for metals in Earth's crust (Lesandrini et al., 2023; Memarian & Doleck, 2023).

The aim of AI was never to harm humans. The aim of AI was never to replace humans and the aim of AI was never to take over the world of humans. The aim of AI was to augment humans, to help humans, to help scientific discoveries, to help humans in case of natural calamities, to help humans in pandemic-like situations, and so on. Other applications where AI seems to insightfully help humans are in day-to-day medical care centers, mechanical engineering companies, driving in semi and fully-automated cars, in bot-based deliveries in dire flood-like situations, in intelligent robotics in various segments of application such as textile engineering to even in running advancements in aircraft, traffic management, and space programs, to mention a few.

But now the development of AI has been at its greatest peak and it can do the work humans are doing in almost all fields. So many jobs are being replaced by AI these days, but that should not fear people. New jobs are created at the same rate as well. However, the statistics for new jobs created versus jobs lost is yet to come out to common people. This is how development has been progressing since the industrial revolution. Getting into a new domain of work because AI has taken away many workflows is not easy. We all remember when the textile engineering department was computerized then so many jobs were taken away. The affected engineers had to take new jobs. Once an area becomes obsolete, a new area of development starts. When mobile phones came, landline phones became obsolete. Today the same mobile phones provide employment to many people all around the globe. More on solutions to job loss is discussed in the coming sections.

The aim of this paper is to present the ethical aspects of AI, its ethical uses, and proposed solutions to problems that arise with the growth of AI and especially AI with Robotics. Section 2 describes the why behind studying AI and Robotics ethical issues. Section 3 discusses Robotics with AI. Section 4 presents the solutions for key ethical problems in AI and Robotics, and Section 5 gives the conclusion of the paper.

1. Preliminary notes on Ethics in AI and Robotics

Many people think of AI as a threat to its useful applications. However, as with other scientific disciplines, AI is a well-grown subject on its own. The need for laying out the rules for Ethics in AI and Robotics is discussed in this paper. It must be known that just like other subjects of science, AI too needs to have certain constraints in its development, discovery, and deployment. This is nothing new, the well-developed subjects such as chemistry, physics, biology, and so on, all have guidelines of use. One example can be some lab-grown fungi, being leaked out and creating havoc in nature; this can be the result of a lack of caretaking and missed protocols of the lab in which fungi were stored for some practical works. Hence, guardrails are laid out in all fields of science and hence should be employed in AI and Robotics as well. Another example is a new car using nuclear energy to run the engines. If not tested well in all extreme temperatures and conditions it can create many mishaps.

The difference between other scientific disciplines and AI is that AI grew from some scientific disciplines primarily consisting of computer science and mathematics, in which there are no protocols for the delivery of products. Hence, it all started with the delivery of AI products without scientific and social guidelines for deployment. Another reason is AI is still a newbie when compared to other subjects; this must be accepted while framing the constraints of products produced with AI.

The good news is there are no major regular faults with AI and Robotics yet. Some problems that occurred a little while back were in autonomous cars and recommender system of a tech giant. The future may develop more AI and Robotics products but those should be ethical, there are the responsibilities of AI. AI has helped humans reach the level of development that exists today. So many devices and products we use, from washing machine to dishwasher to online vacation ticket booking, are rich in one form of AI or another. They are to be used in the future as well. The use of AI cannot be stopped; hence, AI and Robotics need to follow ethics to be used in larger potential.

AI is now an independent subject of its own. What we require now is that AI has its own instruction manuals, just like all physics experiments have pre-defined instructions, likewise all AI and Robotics experiments must have instruction sets. This must be done for each AI application. It may take some time to draw the instruction set, and the hope is, it shall be useful for we are defining the rules scientifically. This compliance of rules shall be tested well before the release of each AI product, be it in Robotics or just in NLP (Rich et al., 2009) tasks that do the recommendation or play a song based on your liking. Hence, proper guidelines for all kinds of AI labs need to be set up.

2. Robotics

The definition of Robotics is extensive and characterization is still bleak. Typically, robots are entities and machines that define mechanical movements and can be with or without any kind of Artificial Intelligence. Robotics is the study of robots (Agarwal & Stoff, 2023). However, this paper shall be focused on smart Robotics (Joachim et al., 2021) equipped with capabilities to run and work on AI-based concepts. The use of robotics can include a wide range from mere mechanical jobs, to robots for medical surgery, to even humanoid robots ready for space discoveries and space travel on their own, but still to be guided in one way or another by human targets.

There are other concerns about the definition of Robots, as in a machine that is remotely guided to perform some tasks. There are discussions on this as well (De Felice et al., 2022), whether such a machine is called an intelligent robot. The answer varies but we consider the answer to be yes, for it is not using a human brain, but signals sent from a distance through the internet or other sources. An example of such devices is IoT-based bots. Hence, these products increase the definition of Robotics, indeed intelligent robotics. They mimic the working of the brain, even if it is through a communication channel. This extends the laws of Ethics in Robotics to be applied to all such devices as well.

Why is Robotics and its analysis important to be considered in AI Ethics discussion? This is because Robotics is the future in which AI is heading to. Robots should always be monitored and altered by humans under whose supervision the assigned task is performed. Here comes ethics for Robotics that use AI. The Ethics for Robotics constitute not only the management of work undertaken but also how the AI-powered Robotics affect its environment actors around the task area.

2.1. Responsible robotics

Responsible robotics (Memarian & Doleck, 2023) is the robotics which aims to help humans in performing tasks that can vary from day-to-day household chores to even complicated surgeries, and even to journeys in space for scientific discoveries. But being a major part of AI, robotics should not harm humans and their environments. This should be the aim with which responsible robotics should be built, this needs to be the foundation stone of building intelligent AI-based Robotics. It must be noted that responsible robotics cannot hither to the other side of wrong impacts given the inputs are modeled into outputs. For this, the ethics protocols need to be made.

Why we need robots is a different question. They are required to do things to help humans or things which humans cannot do. Robots work on programming languages to even bytes and bits-based data. Intelligent robotics needs to understand problems before it can solve them.

Whether we use Robotics (Brooks, 1991) with AI, many kinds of robotics are now in use in industries, MNC companies, and manufacturing. They can be used in rescue operations from a mine in case of some need, to colonize another planet or space object before humans reach a new place in outer space that is not safe for humans. For the safety of humans, robotics needs to be sent to other outer space locations before humans. Yes, people do say "There is no Planet B", that is true now, but mankind progresses with hope, and with hope, humans have reached this advancement in all sectors of development. There is no harm in trying to make AI and Robots that can help the health and well-being of Planet A, which is the Earth while fostering other space bodies for life and needs.

Other areas where AI-based Robots can help are fire-resistant robots to help in extreme forest fires which the firefighters cannot extinguish fire. Robots can take out metals and reusables from garbage and to automatically distinguish single-use plastic from other kinds of garbage. How much can humans do alone? There are jobs not meant for humans, let us accept that. There come AI-based machines and Robots to use. With their use comes the responsibility of humans to make these machines safe for use. Once again, AI is still in its youth and in the nascent stage of development; hence, there should be nothing to fear, as long as ethics are applied to all new or old use cases for AI applications.

3. Solutions for Ethics in AI and Robotics

Once the software is set and a machine always follows the rules inscribed in its software, one can be confident that responsible robotics cannot hither towards the wrong side. There are two characterizations of AI in terms of its use and the outputs it produces. These are given as follows (Kumar et al., 2023):

1. The good AI

The good AI is the beneficial AI, which is developed to accomplish some tasks. It can be tested using black box and white box testing as well. These kinds of AI applications require fixed inputs and produce fixed outputs that are well predictable. These may use typical pattern recognition tools (Duda & Hart, 2006) such as decision tree-based solutions to predict leukemia using a support vector machine. These algorithms cannot do harm to anyone and they typically have predefined output guidelines. Other uses are in defense, aircraft flying, rocket launch, to even healthcare prediction, to operations. Hence, these algorithms are termed as good AI.

2. The bad AI

The AI algorithm can harm by use of bias, privacy sacrifice, bad language, self-esteem or even hurting in any form, and more comes under bad AI. These things materialize in AI as beautifying apps that affect teenagers' self-esteem, video editing by adults, fake profiles, fake images, AI-based agents playing games, fake and manipulated news, hacking with AI, and copywriting issues, to mention some. These can lead to self-harm apart from losses in personal and professional lives.

All major problems that we need solutions for are products of bad AI. Good AI is primarily ethical and does not provide any harmful problems. These typically use machine learning (Bishop, 2006, Palladino, 2023) algorithms to find solutions and work on the problems. Still, to be on the safer side, let the guidelines be made for all kinds of AI, good AI, bad AI or simple AI, or AGI, the general intelligence-based AI. For any of these AI and Robotics with AI need to follow both black box testing and white box testing. The testing can to some extent prevent wrong outputs. Black box testing can be performed by any good computer-literate person, while white box testing is more comprehensive testing that involves getting into the codebase to get the why of an encountered error. This solves the problem from the root. Hence, white box testing should be encouraged in ethical AI and its use in Robotics and IoT.

3.1. Privacy

AI tools such as “Help me write”, “smart compose” and “smart reply” can raise privacy concerns (Zhang et al., 2021; Stahl & Wright, 2018), due to the impression that your emails are being read by AI and can be used in the wrong ways. Privacy does not end with emails. Privacy can extend to data privacy, where data entered by a person is at risk of leaking, and personal privacy where the profile of the AI hardware/software user is at risk. The data can be data about the user’s personal choices or about their company, family, or properties. Moreover, any kind of attack on privacy is wrong, and AI-based tools and apps should be saved from privacy attacks or virus threats. AI apps should be made in such a way as to avoid attacks by viruses. Further, AI apps themselves can generate data from users’ web browsing or other activities; all these should be taken care of before using the AI tool.

The solution to this problem is self-awareness and installing relevant patches on the system that use AI, installing anti-malware and antivirus on systems. For other apps that use AI-based auto-fillers, a toolkit maker must be contacted to appliy the code of conduct for AI tools. This is the only way to gain security over our data.

3.2. Ownership

With the advancements in AI comes the problem of ownership. AI initially was used by artists to help artists, songwriters, scriptwriters, and movie makers but now it has taken over all these domains. Who taught AI all this? The answer is humans. AI-based software was trained on hundreds and thousands of human-created art, photographs, chats and texts. But when AI software creates something new, say a new image file, it may be created using thousands of man-made items This means the credit for new images made by AI to some extent lies in the hands of humans who made the base image, and who made AI learn painting or singing, as the case may be.

The solution to this can be understood as follows. There are traditional artists and AI and digital arts-based artists. Let us understand all this with the help of restricting art to painters; similar analogy would apply to other artists, be they scriptwriters or musicians, to mention a few.

3.2.1. Traditional artists

Traditional artists stick to age-old ways along with newer approaches to make art. Many artists create artwork with traditional colors and styles and may choose acrylic paints while some use tough oil paints. Many artists work with glass or clay. These are all examples of traditional ways of creating art. For them, this art is not only their profession but also their livelihood, passion, and source of love and worship. Most artists work as a hobby and for generating side income; these artists may not be as badly hit as those who rely completely on art for a living.

As with newer developments in AI, new needs, and developments in technology, old ways of making art seem to become obsolete. The newer kinds of art are:

1. Faster to make,
2. Typically cheaper, and
3. More lucrative (Scimeca & Bonfiglio, 2023).

However, most people still prefer the original arts. Traditional kinds take more effort than the competitive digital arts. For many, getting in a new technique is not an easy task to do, and hence they stick to older and typical ways to create art. Initially, digital arts are not easy to grasp either but once an artist is a master of digital art it will not take much hurdles to expertise in it.

3.2.2. Tech and AI artists

The Tech and AI artists are the artists who use some form of technology or AI to make artwork of any kind, be it music, script writing, or painting. These can use tools such as digital art software, 2D or 3D printed art, or may be powered by AI and Robotic hands. These artists take training to learn the toolkits; once learned the artists are free to explore the infinite world of arts that can be made with these toolkits. The AI-powered toolkits are even more interesting to make, though an artist may need to write a few lines of code to generate such masterpieces in music and arts. Here, the artist may be working in collaboration or on their own, and at times an artist works on artwork from scratch and many times they edit the work of other artists to enhance them.

Some of these arts can be made on top of art which are not owned by the group of artists who are making the new art. Then legally the original art owner possesses the rights to his/her art. They own the copywriting of the art and still, there are no stringent laws to take care of this. Here both suffer: the digital artist who has put his or her AI-based art knowledge on someone else's artwork, and the original traditional artist(s) for not getting the

acknowledgment as deserved. Till the time a law comes to this front, an acknowledgment must be paid to the base artist.

The pressure on artists is enormous, both on traditional artists and digital and AI-based artists. The concerns include license of use, earning, owning the rights, publicity, and certificate of authenticity.

3.2.3. Solutions

The AI and Robotics based arts are trained on thousands and more of human-made artworks, photographs, scripts, etc. These training data is used to make newer artwork. But it is not always clear how to find the original makers of artwork from AI-generated art. Sometimes the contribution is just to make a colored ball in the new AI art and many times it is the whole face that is used and maybe processed with a makeup filter. The solution lies in how much of art was taken from original training data, and how much was learned as a teacher-learner relationship. The solution can be legally formulated as follows:

1. The AI artwork has more than 80% of similarity with the original art in training data. Then the original artist and the new AI artist can get into some negotiations on sharing the profit or barring the sale of the new artwork, as the base artist wants. The original artist can buy the work the digital artist made, based on hours spent by the digital artist on editing.

2. In case of less than 80% of similarity, the original artist can claim a share of the profit on selling the artwork and cannot stop the digital artist from selling and purchasing the artwork.

3. In case the original artist wants to work together with a digital-AI artist, they can share the profits and the collaboration can lead to new heights in creating arts never seen before.

Such solutions may make the marketplace for arts ownership a harmonious place to work in.

3.3. Towards Responsible Robotics

The problems with responsible robotics are (Stahl et al., 2023):

1. Competing robots. As Robotics with AI grows, there may appear problems such as the encounter of robots made by two counties. The encounter needs to be peaceful and Robots should not challenge each other but work in harmony without creating global tensions with conflict of interests.

2. Fully Autonomous Robots

These Robots are the decision makers and are fully self-aware as part of Robotics units that materialize the use of AGI (Artificial General Intelligence). AGI-based Robots can

be self-aware and have their own thought processes. These are robots in making and to the best of our knowledge no true AGI-based Robot is out of use or work. Hence, special constraints need to be on AGI-based robots.

3. Malfunction AI-based Robots

These kinds of problems can be a real threat to the proper functioning of the process for which the robot was made. The only way this can be handled is by taking the robot out of work and installing some patches necessary to correct the working. This needs to be followed by proper testing and then re-deployment of the same or new robot at work.

The solution is to make universal machines which are non-competing in the delivery of outcomes and work under the Ethics of the welfare of humans. This makes it mandatory for the talks at the global level for AI and Robotics neutrality, compliance, and laws of use to attain mutually beneficial outputs. Hence, countries around the world should sign in legal documents wherein mutual cooperation is guaranteed both in AI and Robotics. The deal should include robotic entities made by countries, in defense, government, public and private sectors to be declared for use with a global approval.

3.3.1. AI-based Autonomous Cars

An autonomous, or AI-based car needs to not only drive from point A to point B, but must follow traffic rules, as well as drive on roads, get parked, maintain speed limits on different roads, not jump on humans and animals on the way. Only after these things are completed, an autonomous car can be deployed on roads. This needs to be a law. In the past few years an autonomous car bumped on the road into another entity and called it a mistake. As per what AI Ethics should make it a law, such cars should not be employed on roads to run, till all AI-based tests for Ethics are mandated for it.

One must note, no one law can be sufficient for Robotics. Let us understand ethics for autonomous cars with general Robotics ethics implementation. Each field of application of Robotics is different, hence first the definitions need to be made and then applications need to be filled in that states what role AI based Robots shall do, and then the legal team must fill in what all the entities and actors are which the AI Robot can touch in this process, then safety of operation must be made for each department. The ethics team must sit with the Robotics application team and set out guidelines for the safe use of Robotics. Once the company making robots is ready to deploy the robots, the proof of concept should be done by the AI Ethics Standards team. This needs to be through and robots should not be allowed to function till this robotic Proof of Concept is completed (Leeson & Coyne, 2005).

3.3.2. AI, Robotics, and Employment

With AI comes the automation of current fields, which may lead to some job losses. Training and retraining are some solutions. But this is not guaranteed in all areas, and some people cannot retrain, given their age or disability. In such cases, an employer should keep in the account of whom to fire and whom to keep. These are ethical concerns and this is a solution to the side effects of AI doing human work (Duan et al., 2019). There are huge potentials humans can reach, there are so many new fields to explore with both government and private funding. But the transition from one field to a new field should be smooth and companies should help the talent of their company find new jobs of equitable scope, honor, designation, and remuneration. Apart from that, a guarantee of, say, five years of work should be provided. Once again, sensitive people should be reserved in jobs and should not be laid off as in this year's mass layoffs around the world.

There are huge lists of applications that AI and Robotics can perform. All this does not mean job losses and layoffs. Robots installed in cities and countries shall not take away jobs without giving new jobs. Just like making a space for a new pet in the house or a new chandelier does not take away your sleeping time, the same is with AI and Robotics gadgets. This is the only way ahead, to accept the change AI and Robotics have brought and to wait for new arenas to be built for new jobs. At the same time, all should be done carefully while following the constraints of AI which follows Ethics (Hellwig et al., 2019).

3.3.3. AI-based Language Models

There are huge applications of AI in Large Language Models (LLM), and the past year saw the growth of AI LLM models like never before (Ferreira & Lipoff, 2023, Glaser et al., 2019). One after the other models came to the limelight breaking each other's records in performance and problem-solving and some in both. The problems that come with LLMs are the prediction of outputs, bias, privacy issues, wrong content, and bad language, to mention a few (Díaz-Rodríguez et al., 2023). The way forward for LLMs should require white box-style evaluations of AI software, as was discussed at the beginning of this section. White box testing should help predict the next output with a given input combination. This should minimize problems like those that happened in a tech giant two years ago when its wrong recommendation system affected many groups of people.

Conclusions

Once the software is set and well tested, a machine always follows the rules inscribed in its software, and one can be confident that responsible Robotics with AI cannot hither towards the wrong side. In this paper, we discussed many ethical issues existing in the current

scenario. Further, novel solutions were provided for these ethical issues. Moreover, the combination of Robotics with AI was discussed for its potential use and for its ethics for upcoming combinations of Robotics with AI. Many more areas of ethics need devised solutions, which is part of the future work of the author.

References

Agarwal, A., & Stoff, B. (2023). Ethics of using generative pretrained transformer and artificial intelligence systems for patient prior authorizations. *Journal of the American Academy of Dermatology*, *20*, 23–34. https://doi.org/10.1016/j.jaad.2023.04.030

Bishop, C. M. (2006). *Pattern recognition and machine learning*. New York: Springer. https://clck.ru/37AU6Z

Brooks, R. A. (1991). New approaches to robotics. *Science*, *253*(5025), 1227–1232.

Critchlow, A. J. (1985). *Introduction to robotics*. Macmillan Pub Co.

De Felice, F., Petrillo, A., De Luca, C., & Baffo, I. (2022). Artificial Intelligence or Augmented Intelligence? Impact on our lives, rights and ethics. *Procedia Computer Science*, *200*, 1846–1856. https://doi.org/10.1016/j.procs.2022.01.385

Hellwig, J., Huggett, S., & Siebert, M. (2019). *Artificial Intelligence: How knowledge is created, transferred, and used*. Elsevier. https://doi.org/10.17632/7ydfs62gd6.2

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, 101896. https://doi.org/10.1016/j.inffus.2023.101896

Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2019). Artificial intelligence for decision making in the era of Big Data – evolution, challenges, and research agenda. *International Journal of Information Management*, *48*, 63–71. https://doi.org/10.1016/j.ijinfomgt.2019.01.021

Duda, R. O., & Hart, P. E. (2006). *Pattern classification*. John Wiley & Sons.

Ferreira, A. L., & Lipoff, J. B. (2023). The complex ethics of applying ChatGPT and language model artificial intelligence in dermatology. *Journal of the American Academy of Dermatology*, *89*(4), e157-e158. https://doi.org/10.1016/j.jaad.2023.05.054

Glaser, J. I., Benjamin, A. S., Farhoodi, R., & Kording, K. P. (2019). The roles of supervised machine learning in systems neuroscience. *Progress in Neurobiology*, *175*, 126–137. https://doi.org/10.1016/j.pneurobio.2019.01.008

Joachim von Braun, Margaret S. Archer, Gregory M. Reichberg, & Marcelo Sánchez Sorond. (2021). AI, Robotics, and Humanity: Opportunities, Risks, and Implications for Ethics and Policy. In J. von Braun et al. (Eds.), *Robotics, AI, and Humanity*. https://doi.org/10.1007/978-3-030-54173-6_1

Kumar, P., Chauhan, S., & Kumar, L. A. (2023). Artificial Intelligence in Healthcare: Review, Ethics, Trust Challenges & Future Research Directions. *Engineering Applications of Artificial Intelligence*, *120*, 105894. https://doi.org/10.1016/j.engappai.2023.105894

Leeson, P. T., & Coyne, C. J. (2005). The economics of computer hacking. *JL Econ. & Pol'y*, *1*, 511.

Lesandrini, J., Idris, M. Y., & Reis, D. S. (2023). The Ethics of Artificial Intelligence and Machine Learning. *Journal of Radiology Nursing*, *42*(3), 265–266. https://doi.org/10.1016/j.jradnu.2023.05.001

Memarian, D., & Doleck, T. (2023). Fairness, Accountability, Transparency, and Ethics (FATE) in Artificial Intelligence (AI) and higher education: A systematic review. *Computers and Education: Artificial Intelligence*, *5*, 100152, https://doi.org/10.1016/j.caeai.2023.100152

Mueller, V. C. (2012). Introduction: philosophy and theory of artificial intelligence. *Minds and Machines*, *22*(2), 67–69. https://doi.org/10.1007/s11023-012-9278-y

Palladino, N. (2023). A 'biased' emerging governance regime for artificial intelligence? How AI ethics get skewed moving from principles to practices. *Telecommunications Policy*, *47*(5), 102479. https://doi.org/10.1016/j.telpol.2022.102479

Rich, E., Knight, K., & Nair, S. (2009). *Artificial Intelligence*. Tata McGraw Hill.

Saveliev, A. M., Zhurenkov, D. A., Poikin, A. E., & Berkutova, T. A. (2021). Ethics of Artificial Intelligence and Post-non-classical Scientific Rationality. *IFAC-PapersOnLine*, *54*(13), 397–401. https://doi.org/10.1016/j.ifacol.2021.10.480

Schank, R. C. (1991). Where's the AI? *AI magazine*, *12*(4), 38. https://doi.org/10.1609/aimag.v12i4.917

Scimeca, M., & Bonfiglio, R. (2023). Comment on redefining authorship in the era of artificial intelligence: balancing ethics, transparency, and progress. *ESMO Open*, *8*(5), 101635. https://doi.org/10.1016/j.esmoop.2023.101635

Stahl, B. C., & Wright, D. (2018). Ethics and privacy in AI and big data: Implementing responsible research and innovation. *IEEE Security & Privacy*, *16*(3), 26–33. https://doi.org/10.1109/msp.2018.2701164

Stahl, B. C., Brooks, L., Hatzakis, T., Santiago, N., & Wright, D. (2023). Exploring ethics and human rights in artificial intelligence – A Delphi study. *Technological Forecasting and Social Change*, *191*, 122502. https://doi.org/10.1016/j.techfore.2023.122502

Stahl, B. C. (2021). Perspectives on Artificial Intelligence. In *Artificial Intelligence for a Better Future. SpringerBriefs in Research and Innovation Governance* (pp. 7–17). Springer, Cham. https://doi.org/10.1007/978-3-030-69978-9_2

Turing, A. M. (2009). *Computing machinery and intelligence* (pp. 23–65). Springer Netherlands.

Xiao-Fan, L., Zhaoyang, W., Wei, Zh., Guoyu, L., & Gwo-Jen, H. (2023). Technological support to foster students' artificial intelligence ethics: An augmented reality-based contextualized dilemma discussion approach. *Computers & Education*, *201*, 104813. https://doi.org/10.1016/j.compedu.2023.104813

Zhang, Y., Wu, M., Yijun Tian, G., Zhang, G., & Lu, J. (2021). Ethics and privacy of artificial intelligence: Understandings from bibliometrics. *Knowledge-Based Systems*, *222*, 106994. https://doi.org/10.1016/j.knosys.2021.106994

Author information

Yadav Nidhika – Ph.D., Independent Researcher
Address: Chattarpur Enclave Phase II Delhi-110074, India
E-mail: yadavnidhika68@gmail.com
ORCID ID: https://orcid.org/0000-0002-0165-6453
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57195398958
WoS ID: https://www.webofscience.com/wos/author/record/2269009
Google Scholar ID: https://scholar.google.com/citations?user=fndffSwAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – July 23, 2023
Date of approval – October 25, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:17:296.41:004.8
EDN: https://elibrary.ru/mdiefv
DOI: https://doi.org/10.21202/jdtl.2023.41

Этика искусственного интеллекта и робототехники: ключевые проблемы и современные способы их решения

Нидика Ядав

Независимый исследователь
г. Нью-Дели, Индия

Ключевые слова

ChatGPT,
безопасность,
искусственный интеллект,
кибербезопасность,
конфиденциальность данных,
право,
робот,
робототехника,
цифровые технологии,
этика

Аннотация

Цель: современные достижения в области развития и распространения цифровых технологий привлекли внимание ученых и практиков к обсуждению ключевых этических проблем, связанных с искусственным интеллектом и робототехникой, в связи с чем в настоящем исследовании представлены результаты этой дискуссии и обозначены наиболее актуальные задачи, решение которых определяет пути совершенствования регулирования искусственного интеллекта и робототехники в части морализации технологий.

Методы: в процессе исследования использовались практико- и риск-ориентированный подходы, дополняемые мультидисциплинарным анализом документов (европейских принципов и кодексов этики) и исследований, в том числе посвященных различным проблемам искусственного интеллекта и робототехники.

Результаты: в статье обозначены ключевые этические проблемы в области искусственного интеллекта и робототехники; установлено, что затрагиваемые ключевые этические проблемы могут быть решены при условии, если они получат юридическое оформление и будут реализованы на международном уровне; предложенный автором алгоритм, основанный на анализе практики применения цифровых технологий, позволит усовершенствовать нравственные действия технологий при принятии ими решений.

Научная новизна: в данной статье представлены новейшие этические проблемы, которые волнуют ученых и практиков в области искусственного интеллекта и робототехники, и методы их решения этико-правовыми средствами, направленными на морализацию технологий и повышение ее ответственности.

Практическая значимость: все решения, представленные в статье, имеют практическое значение и готовы к широкому внедрению на международном уровне. Их оформление в нормативном виде и последующее соблюдение приведут к уменьшению вреда, который может нанести искусственный интеллект в прикладных областях, в том числе в робототехнике с использованием искусственного интеллекта. В связи с этим нормативные, в том числе законодательные, решения должны быть приняты как можно скорее, чтобы искусственный интеллект и робототехника приобрели статус надежных инструментов при использовании этих систем на работе, дома и в других сферах, таких как торговые центры, магазины, школы, университеты и т. д.

Для цитирования

Ядав, Н. (2023). Этика искусственного интеллекта и робототехники: ключевые проблемы и современные способы их решения. *Journal of Digital Technologies and Law*, *1*(4), 955–972. https://doi.org/10.21202/jdtl.2023.41

Список литературы

Agarwal, A., & Stoff, B. (2023). Ethics of using generative pretrained transformer and artificial intelligence systems for patient prior authorizations. *Journal of the American Academy of Dermatology*, *20*, 23–34. https://doi.org/10.1016/j.jaad.2023.04.030

Bishop, C. M. (2006). *Pattern recognition and machine learning*. New York: Springer. https://clck.ru/37AU6Z

Brooks, R. A. (1991). New approaches to robotics. *Science*, *253*(5025), 1227–1232.

Critchlow, A. J. (1985). *Introduction to robotics*. Macmillan Pub Co.

De Felice, F., Petrillo, A., De Luca, C., & Baffo, I. (2022). Artificial Intelligence or Augmented Intelligence? Impact on our lives, rights and ethics. *Procedia Computer Science*, *200*, 1846–1856. https://doi.org/10.1016/j.procs.2022.01.385

Hellwig, J., Huggett, S., & Siebert, M. (2019). *Artificial Intelligence: How knowledge is created, transferred, and used*. Elsevier. https://doi.org/10.17632/7ydfs62gd6.2

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, 101896. https://doi.org/10.1016/j.inffus.2023.101896

Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2019). Artificial intelligence for decision making in the era of Big Data – evolution, challenges, and research agenda. *International Journal of Information Management*, *48*, 63–71. https://doi.org/10.1016/j.ijinfomgt.2019.01.021

Duda, R. O., & Hart, P. E. (2006). *Pattern classification*. John Wiley & Sons.

Ferreira, A. L., & Lipoff, J. B. (2023). The complex ethics of applying ChatGPT and language model artificial intelligence in dermatology. *Journal of the American Academy of Dermatology*, *89*(4), e157-e158. https://doi.org/10.1016/j.jaad.2023.05.054

Glaser, J. I., Benjamin, A. S., Farhoodi, R., & Kording, K. P. (2019). The roles of supervised machine learning in systems neuroscience. *Progress in Neurobiology*, *175*, 126–137. https://doi.org/10.1016/j.pneurobio.2019.01.008

Joachim von Braun, Margaret S. Archer, Gregory M. Reichberg, & Marcelo Sánchez Sorond. (2021). AI, Robotics, and Humanity: Opportunities, Risks, and Implications for Ethics and Policy. In J. von Braun et al. (Eds.), *Robotics, AI, and Humanity*. https://doi.org/10.1007/978-3-030-54173-6_1

Kumar, P., Chauhan, S., & Kumar, L. A. (2023). Artificial Intelligence in Healthcare: Review, Ethics, Trust Challenges & Future Research Directions. *Engineering Applications of Artificial Intelligence*, *120*, 105894. https://doi.org/10.1016/j.engappai.2023.105894

Leeson, P. T., & Coyne, C. J. (2005). The economics of computer hacking. *JL Econ. & Pol'y*, *1*, 511.

Lesandrini, J., Idris, M. Y., & Reis, D. S. (2023). The Ethics of Artificial Intelligence and Machine Learning. *Journal of Radiology Nursing*, *42*(3), 265–266. https://doi.org/10.1016/j.jradnu.2023.05.001

Memarian, D., & Doleck, T. (2023). Fairness, Accountability, Transparency, and Ethics (FATE) in Artificial Intelligence (AI) and higher education: A systematic review. *Computers and Education: Artificial Intelligence*, *5*, 100152, https://doi.org/10.1016/j.caeai.2023.100152

Mueller, V. C. (2012). Introduction: philosophy and theory of artificial intelligence. *Minds and Machines*, *22*(2), 67–69. https://doi.org/10.1007/s11023-012-9278-y

Palladino, N. (2023). A 'biased' emerging governance regime for artificial intelligence? How AI ethics get skewed moving from principles to practices. *Telecommunications Policy*, *47*(5), 102479. https://doi.org/10.1016/j.telpol.2022.102479

Rich, E., Knight, K., & Nair, S. (2009). *Artificial Intelligence*. Tata McGraw Hill.

Saveliev, A. M., Zhurenkov, D. A., Poikin, A. E., & Berkutova, T. A. (2021). Ethics of Artificial Intelligence and Post-non-classical Scientific Rationality. *IFAC-PapersOnLine*, *54*(13), 397–401. https://doi.org/10.1016/j.ifacol.2021.10.480

Schank, R. C. (1991). Where's the AI? *AI magazine*, *12*(4), 38. https://doi.org/10.1609/aimag.v12i4.917

Scimeca, M., & Bonfiglio, R. (2023). Comment on redefining authorship in the era of artificial intelligence: balancing ethics, transparency, and progress. *ESMO Open*, *8*(5), 101635. https://doi.org/10.1016/j.esmoop.2023.101635

Stahl, B. C., & Wright, D. (2018). Ethics and privacy in AI and big data: Implementing responsible research and innovation. *IEEE Security & Privacy*, *16*(3), 26–33. https://doi.org/10.1109/msp.2018.2701164

Stahl, B. C., Brooks, L., Hatzakis, T., Santiago, N., & Wright, D. (2023). Exploring ethics and human rights in artificial intelligence – A Delphi study. *Technological Forecasting and Social Change*, *191*, 122502. https://doi.org/10.1016/j.techfore.2023.122502

Stahl, B. C. (2021). Perspectives on Artificial Intelligence. In *Artificial Intelligence for a Better Future. SpringerBriefs in Research and Innovation Governance* (pp. 7–17). Springer, Cham. https://doi.org/10.1007/978-3-030-69978-9_2

Turing, A. M. (2009). *Computing machinery and intelligence* (pp. 23–65). Springer Netherlands.

Xiao-Fan, L., Zhaoyang, W., Wei, Zh., Guoyu, L., & Gwo-Jen, H. (2023). Technological support to foster students' artificial intelligence ethics: An augmented reality-based contextualized dilemma discussion approach. *Computers & Education*, *201*, 104813. https://doi.org/10.1016/j.compedu.2023.104813

Zhang, Y., Wu, M., Yijun Tian, G., Zhang, G., & Lu, J. (2021). Ethics and privacy of artificial intelligence: Understandings from bibliometrics. *Knowledge-Based Systems*, *222*, 106994. https://doi.org/10.1016/j.knosys.2021.106994

Информация об авторе

Ядав Нидика – PhD, независимый исследователь
Адрес: 110074, Индия, г. Дели, Чаттапур Анклав Фейз II
E-mail: yadavnidhika68@gmail.com
ORCID ID: https://orcid.org/0000-0002-0165-6453
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57195398958
WoS ID: https://www.webofscience.com/wos/author/record/2269009
Google Scholar ID: https://scholar.google.com/citations?user=fndffSwAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов

Финансирование

Исследование не имело спонсорской поддержки

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.41.51 / Охрана авторских прав
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 23 июля 2023 г.
Дата одобрения после рецензирования – 25 октября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.42

Achieving Algorithmic Transparency and Managing Risks of Data Security when Making Decisions without Human Interference: Legal Approaches

Anna K. Zharova

Institute of State and Law of the Russian Academy of Sciences
Moscow, Russian Federation

Keywords

algorithmic transparency,
artificial intelligence,
confidentiality,
data protection,
data security,
digital technologies,
GDPR,
information technologies,
law,
personal data

Abstract

Objective: to compare modern approaches in law to the use of program codes and algorithms in decision-making that meet the principles of transparency and openness, as well as the increasingly stringent requirements for ensuring the security of personal and other big data obtained and processed algorithmically.

Methods: the main methods for researching the principle of transparency in algorithmic decision-making were formal-legal and comparative analysis of legal acts and international standards of information security, as well as the principles and legal constructions contained in them.

Results: it was determined that the development of information security standardization, inclusion in legal acts of requirements for the development of information technologies that comply with the principles of transparency and openness of applied algorithms will minimize the risks associated with the unlawful processing of users' big data and obtaining information about their privacy. Proposals were identified, related to the implementation of algorithmic transparency in the field of data processing legal regulation. Recommendations were formulated, based on which the legislator can solve the problem of ensuring the openness of the logic of information technology algorithms with regard to modern standards of information security.

Scientific novelty: it consists in the substantiation of new trends and relevant legal approaches, which allow revealing the logic of data processing by digital and information technologies, based on the characterization of European standards of the "privacy by design" concept in new digital and information technologies of decision-making and data protection, as well as on the new legal requirements for artificial intelligence systems, including the requirement to ensure algorithmic transparency, and criteria for personal data and users' big data processing. This said, data protection is understood as a system of legal, technical and organizational principles aimed at ensuring personal data confidentiality.

Practical significance: it is due to the need to study the best Russian and international practices in protecting the privacy of users of digital and information technologies, as well as the need for legislative provision of requirements for the use of algorithms that meet the principles of transparency and openness of personal data processing, taking into account the need to ensure confidentiality at all stages of the life cycle of their processing, which will ensure the continuity of security management.

For citation

Zharova, A. K. (2023). Achieving Algorithmic Transparency and Managing Risks of Data Security when Making Decisions without Human Interference: Legal Approaches. *Journal of Digital Technologies and Law, 1*(4), 973–993. https://doi.org/10.21202/jdtl.2023.42

Contents

Introduction

Information technology models are becoming increasingly complex, and more and more human-related data is being processed by them. For example, the technologies of the Internet of Things collect a large amount of data, which may contain various types, including users' big data. A user of information technologies (further – IT) is concerned about the impossibility to control the actions performed by information technologies, as well as the inability to understand the logic of the algorithms processing their data, what data are processed and what the final result of data analysis is. The desire to understand the criteria for analyzing processed data, as well as the need to ensure control over the list of such data, have led the legislator to the idea of including in legal acts the requirement to use algorithms that meet the principles of transparency and openness. In other words, it is necessary to reveal the logic of data processing by information technologies.

In computer science, the term "algorithmic transparency" is used to describe the transparency of processes occurring during the information technologies functioning. Due to the need to ensure the protection of user data, this term was borrowed by legal science.

In the Russian legislation, the term "algorithmic transparency" is used to describe the regulation of relations occurring during the application of artificial intelligence systems (further – AI)[1]. However, researchers believe that the term "algorithmic transparency" can be used to describe a wider range of relations that go beyond AI functioning (Kuteinikov et al., 2020; Gulemin, 2022).

Due to such polysemy, it is first of all necessary to study the "algorithmic transparency" concept, and then, based on the obtained results, to research the proposals related to the algorithmic transparency implementation in the field of legal regulation of data processing.

1. Notion of algorithmic transparency

The Concept of developing the regulation of relations in the sphere of artificial intelligence and robotics up to 2024[2] refers the problem of algorithmic transparency of artificial intelligence systems to the conceptual problem areas of regulation of relations in the said sphere[3].

"Algorithmic transparency" of the information model allows understanding the logic of the information model functioning implemented by AI with the given input data. However, it is essential that the AI algorithms complexity does not allow any AI algorithm to be described in such a way that its logic becomes understandable to an average person. The algorithmic

1 Decree of the President of the Russian Federation No. 490 of 10.11.2019 (with the National Strategy for the Development of Artificial Intelligence up to 2030). (2019). Collection of legislation of the Russian Federation, 41, Art. 5700.

2 Order of the Government of the Russian Federation No. 2129-r of 19.08.2020. (2020). Collection of legislation of the Russian Federation, 35, Art. 5593.

3 Ibid.

stages are the most easily perceived in a linear AI model and its mathematical interpretation. The most difficult for understanding is the logic of AI model functioning in a deep AI architecture[4].

In other words, algorithmic transparency is the explainability of the work of "AI and the process of it achieving results, non-discriminatory access of the users of products, created using artificial intelligence technologies, to information about the work of artificial intelligence algorithms applied in these products"[5]. Some researchers believe that technological developments in AI and algorithms have become an integral part of public administration (Feijóo et al., 2020; Carlsson & Rönnblom, 2022; Balasubramaniam et al., 2023; Green, 2022).

2. Can user data be protected through understanding the logic of data processing algorithm?

In 1999, L. Lessig was one of the first authors who, paying tribute to legal and social norms in providing legal regulation of relations arising in the ICT sphere, recognized the software code as an equal component in regulating information relations. A program code defines the ICT space architecture and allows achieving the best result in regulating relations arising in the information sphere (Lessig, 1999).

A program code formalizes the logic of algorithm operation. Proposals to provide algorithmic transparency in software are increasingly common. "Transparency of algorithms becomes a type of control, and transparency of algorithmic decision-making serves to ensure that unfair discriminations can be detected and challenged" (Talapina, 2020). However, there is an opposing point of view. For example, some scholars believe that the requirement of algorithmic transparency is aimed at IT developers' interaction with the authorities in order to normalize citizens' behavior (Wang, 2022).

In our opinion, the algorithmic transparency requirement will not bring the desired result, since it is not always possible even for a specialist to comprehend the logic of an AI algorithm. In this regard, unfair discriminations embedded in AI algorithms cannot always be detected and challenged.

Analyzing the tendency of algorithmic transparency implementation, we will attempt to present positions for and against the algorithm logic disclosure.

---

4 Koreshkova, T. (2020, December 29). Explainable artificial intelligence. GRFC Scientific-technical center. https://clck.ru/36h6w6

5 Decree of the President of the Russian Federation No. 490 of 10.11.2019 (with the National Strategy for the Development of Artificial Intelligence up to 2030). (2019). Collection of legislation of the Russian Federation, 41, Art. 5700.

An average person, hoping for the algorithm logic disclosure, believes it will allow them to understand that logic. However, such proposals, although not groundless, have their disadvantages. Firstly, for the majority of people incompetent in the field of programming and information technology development, the algorithm logic disclosure will not provide any information. Secondly, if the algorithm (for example, an AI) user understands its logic, they will be unable to change the algorithm because this will require revision of the entire mathematical toolkit embedded therein. Thirdly, the algorithm logic disclosure must not contradict the intellectual property law, since the intellectual rights to algorithms belong to its developers. Accordingly, the algorithm logic disclosure may occur in strictly limited cases only.

Other researchers suggest replacing the algorithm logic disclosure with insurance of risks associated with information security. For example, a user boarding an airplane and entrusting their life to a carrier does not study the logic of the airplane software beforehand. All risks are assumed by the carrier, an insurer and other persons responsible for passenger transportation (Ostroumov, 2015). Cannot we use the same legal framework of regulating relations in the case of data processing?

"Carriers" of user data are various information intermediaries like providers and operators of personal data processing. Taking into account the high probability that algorithm logic disclosure will actually give nothing to the user, would not it be more effective to apply an insurance system to relations in the ICT sphere, as in the case of air transportation? In this case, the risks of "loss" or unauthorized access to user data, as well as the liability of information intermediaries or personal data operators would be insured.

However, there are pitfalls in this case as well. For example, in the case of air transportation, all stages from the creation of an airplane to its flight are strictly regulated by legal and technical norms. This is not so with the creation of algorithms, information models and their use. Standardization of information technologies to ensure information security is voluntary. Only such information systems as critical information infrastructure of the Russian Federation and systems processing personal data are subject to mandatory standardization.

In this connection, drawing an analogy between ensuring IT user security through algorithmic transparency and air transportation security is only possible in case of using legal and technical norms fro strict regulation of IT creation and its use.

Trust in the field of information security occupies the minds of scholars from different countries (Bujold et al. 2022; Cui et al., 2022; Zhu et al., 2023). Trust is defined as a cultural value that may sometimes conflict with national AI policies (Li, 2022; Robinson, 2020; Xu et al., 2022).

3. Comparative analysis of the principles of algorithmic transparency

Experts from the Community for Fairness, Accountability, and Transparency in Machine Learning (FAT) define five principles of algorithmic transparency – Fairness, Auditability, Explainability, Responsibility and Accuracy[6]. As one may see, the explainability of AI logic is only ranked third in these proposals. This is probably due to the fact that algorithmic openness may not solve the issues of IT user security in all cases.

Researchers propose to supplement these five principles with the principle of making changes to the AI algorithm's operating logic in case of disagreement with its functioning (Malyshkin, 2019; Gordon et al., 2022). However, such proposals raise concerns, as in this case it is possible to violate intellectual property laws. Most companies are reluctant to disclose their algorithms and make them transparent, "citing potential gaming by users that may negatively affect the algorithm's predictive power" (Qiaochu et al., 2020; Stahl et al., 2022).

For our part, we would like to emphasize that the absence in the formulated five principles of "the possibility of changing the AI logic" is understandable. Such algorithms are developed by a team of programmers; changing the logic of operation of one part of an AI algorithm will make the mathematical model of the whole algorithm inoperable (Varsha, 2023; Lang & Shan, 2000; Akter et al., 2022). If the human brain could solve the problem of processing large, unstructured data, AI algorithms would be useless.

In the Russian Federation, in accordance with the National Strategy for the AI development up to 2030, the mandatory principles of AI development and use are: protection of human rights and freedoms, technological sovereignty, integrity of the innovation cycle, reasonable frugality, support for competition, security, and transparency[7].

Security is understood as "inadmissibility of the use of artificial intelligence with the objective of intentionally causing harm to citizens and legal entities, as well as prevention and minimization of risks of negative consequences of the use of artificial intelligence technologies"[8]. Transparency is defined as "explainability of the work of artificial intelligence and the process of achieving its results, non-discriminatory access of the users of products created with the use of artificial intelligence technologies to information about the algorithms of artificial intelligence used in these products" (p. 19)[9].

It should be emphasized that while the Community for Fairness, Accountability and Transparency in Machine Learning defines algorithmic transparency through five

6 Principles for Accountable Algorithms and a Social Impact Statement for Algorithms. https://clck.ru/36h7GL

7 Decree of the President of the Russian Federation No. 490 of 10.11.2019 (with the National Strategy for the Development of Artificial Intelligence up to 2030). (2019). Collection of legislation of the Russian Federation, 41, Art. 5700.

8 Ibid.

9 Ibid.

principles, the Russian legislation has included algorithmic transparency in the principles of AI development and use. The principle of non-discriminatory access of AI users to information about the AI algorithms applied overlaps with the principles formulated by the FAT Community.

The Russian legislation also does not contain the requirement to publish rules defining the basic algorithmic processing of user data, unlike the legislation of France. In accordance with the French Law "On the digital republic" of October 7, 2016, such rules must be published on a public authority website (Talapina, 2020).

In the European Union, the security of personal data of EU residents (Su et al., 2023), as well as the transparency of their processing by algorithms (Matheus et al., 2021; Kempeneer, 2021), including AI (Kempeneer et al., 2023; de Bruijn et al., 2022), is regulated by the General Data Protection Regulation (further – GDPR) (Stöger et al., 2021), which entered into force in 2018 (Mourby et al., 2021).

4. Elaboration and adoption of the General Data Protection Regulation

Although privacy protection is not directly related to personal data protection, the use of personal data allows for the identification of an individual and, consequently, the acquisition of information about his or her private life. Thus, well-protected personal data reduces the risks of obtaining information about a person's private life (Bolton et al., 2021; Leerssen, 2023). The need to combat various breaches of personal data and individual's privacy legislation and to minimize the consequences of such breaches led to the GDPR development and adoption (Willems et al., 2022; Custers & Heijne, 2022).

One of the first cases involving an unlawful acquisition of information about an individual's privacy through illegal access to a personal data base was the Uber case. The Uber's database was hacked in 2014 and 2016, allowing attackers to track the real-time location of every Uber user. In 2017, the Federal Trade Commission (FTC) accused Uber of failing to properly control employees' access to Uber user and driver databases, as well as breaching its information security system. Uber and the FTC subsequently signed an agreement, according to which Uber committed to conducting third-party audits for twenty years and implementing a privacy protection program[10].

In 2017, the FTC included additional provisions in the agreement obliging Uber to audit their system and submit reports to the FTC, as well as to disclose the fees and terms of agreements between Uber and the third parties that monitor vulnerabilities in Uber's software. Under the latest version of the agreement, Uber:

[10] Uber criminal complaint raises the stakes for breach response. https://clck.ru/37AXba

– may be subject to civil penalties if it fails to notify the FTC of incidents involving unauthorized access to Uber user and driver information;

– is prohibited from misrepresenting the system's level of information protection, the privacy, security, and integrity of personal information, and how it controls internal access to consumers' personal information;

– must implement a comprehensive privacy program and receive biennial, independent third-party assessments of the security of its information system for 20 years. Uber must submit these assessments to the FTC and confirm compliance with the adopted privacy program, while the latter must contain the security terms stipulated in its agreement with the FTC;

– must store user location information on the system, protected by a password and encryption;

– must provide annual training to employees responsible for handling personal information on its data protection and security practices and apply the latest security control techniques;

– must use the best data protection practices to protect drivers' personal information;

– must designate one or more employees to coordinate and oversee the security and privacy program, and conduct regular evaluations of the effectiveness of its internal controls and procedures related to the protection of personal and geographic location information of its employees and customers;

– is obliged to use multi-factor authentication before any employee can access sensitive customer personal information, as well as to use other strong data security practices[11].

In connection with the breaches that occurred in 2014 and 2016, Uber paid a $148 million fine[12]. On August 20, 2020, a criminal case was filed against its former chief security officer, charging him with obstruction of justice and allegedly attempting to cover up a data breach that occurred in 2016.

5. Implementation of the General Data Protection Regulation

GDPR defines the every person's right to protection of their personal data in accordance with part 1 of Article 16 of the Treaty on the Functioning of the European Union (TFEU)[13] and

11 Ibid.

12 Uber to Pay $148 Million Fine for Massive Data Breach That Exposed 57 Million Users' Personal Info. https://clck.ru/36h7RG

13 Treaty on the Functioning of the European Union [Rus., Eng.] (with the «List stipulated by Art. 38...", "Overseas countries and territories to which the provisions of Part Four of the Treaty apply...") (signed in Rome on 25.03.1957) (amended and restated as of 13.12.2007). SPS KonsultantPlyus.

part 1 of Article 8 of the Charter of Fundamental Rights of the European Union[14] (further – the Charter) [15], as well as the "right to privacy" (Article 7 of the Charter) [16].

GDPR requires from the companies processing personal data of EU residents or conducting their activities in the territory of EU states to comply not only with legal requirements, but also with organizational and technical requirements. This must be taken into account by developers at the stage of designing information technologies, and is called "privacy in design" (Article 3 of GDPR). The requirement to ensure privacy in the digital world through "privacy by design and by default" is approved by the European Data Protection Board (EDPB) in Guidelines 4/2019 on Article 25 Data Protection by Design and by Default[17].

The implementation of these requirements has raised many questions among companies about their implementation procedures. Therefore, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have provided clarifications. EDPB Statement 03/2021 "Privacy Regulation", adopted by the Privacy and Confidentiality Board for Electronic Communications Services, states that the proposed Regulation should not under any circumstances reduce the level of protection defined in the current Directive 2002/58/EC[18]. The Regulation should complement GDPR by providing additional strong privacy safeguards and protection for all types of electronic communications[19]. Directive 2002/58/EC covers the processing of personal data and privacy protection, including requirements to ensure the security of networks and services; confidentiality of communications; access to stored data; processing of traffic and location data; identification; publicly available subscriber directories, and prohibition of commercial communications (spam)[20]. EDPB pays special attention to the security of personal data processed by employers. It clearly defines the instances and conditions under which employers may access employees' personal data, as well as liability for excessive data collection through data analysis and processing technologies. It includes, for example, an employer using geolocation systems and technologies to continuously monitor an employee's movements and behavior.

---

14 Charter of Fundamental Rights of the European Union (2007/C 303/01) [Rus., Eng.] (with "Explanations..." (2007/C 303/02)) (adopted in Strasbourg on 12.12.2007). SPS KonsultantPlyus.

15 Ibid.

16 Charter of Fundamental Rights of the European Union. https://clck.ru/36h7Tn

17 Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020. https://clck.ru/36h7Ug

18 E-privacy Directive 2009/136/EC. https://clck.ru/36h7VG

19 Statement 03/2021 on the ePrivacy Regulation Adopted on 9 March 2021. https://clck.ru/36h7WF

20 E-privacy Directive 2009/136/EC. https://clck.ru/36h7VG

Since EDPB and EDPS functions overlap, a Memorandum of Understanding[21] between EDPB and EDPS was adopted to differentiate their activities, according to which EDPB ensures the integrity of GDPR law enforcement practice, and EDPS ensures the common approaches of national supervisory authorities. At the same time, EDPB and EDPS may issue joint documents on personal data protection issues.

6. "Privacy by design" concept of information technologies

The "privacy by design" concept was developed long before the GDPR adoption. In 1995, the Data Protection Directive 95/46 / EC[22] included a provision that "to protect data security, technical and organizational measures shall be defined and adopted at the stage of planning the data processing system" (Article 46 of Directive 95/46 / EC).

On June 22, 2011, EDPS put forward the concept of changing the approach to the regulation of personal data protection and privacy[23] as a public opinion of this organization. Given the necessity and appropriateness of taking into account the requirements of personal data protection through privacy by design, the scholars proposed a change in the concept of personal data protection, outlining it in the following seven principles[24]:

1. Privacy by design measures should be preventive and take into account possible risks and threats, rather than being a reactive response to privacy breaches.

2. Privacy solutions for information systems should be implemented in the system at the design level, rather than being an option for the user.

3. Possible risks and threats should be considered at the technology design stage, as well as be stipulated in information security standards and take into account the data context. Personal data security methods should be continuously updated.

4. Confidentiality should be implemented at all stages of the personal data processing life cycle, as it will ensure the continuity of security management. The applied security standards should guarantee the confidentiality, integrity and availability of personal data throughout their life cycle, as well as the implementation of secure data destruction, encryption, access control and logging.

5. Privacy policies and procedures shall be monitored, evaluated and enforced; openness and transparency shall be maintained, in order to meet the principle of accountability and enable the trust of personal data subjects and counterparties,

21 Memorandum of Understanding. https://clck.ru/36h7ic

22 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://clck.ru/36h7jM

23 The History of the General Data Protection Regulation. https://clck.ru/36h7jw

24 The Seven Principles. https://goo.su/mn8ob7

as well as to harmonize business practices. Information on personal information management policies and practices, compliance and grievance mechanisms should be available to individuals.

6. There should be no compromising between security and functionality.

7. The rights and interests of personal data subjects should be the basis for privacy design.

These principles were among the first to take into account virtually all possible risks of a personal data processing breach. However, other concepts have also been proposed[25].

7. Notions of "personal data" and "privacy" in compliance with the EU legislation

In accordance with GDPR, personal data means any information relating to an identifiable natural person. In accordance with Article 4 of the GDPR, such data may include, for example, a reference to an identifier such as name, identification number, location data, online identifier, any factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The GDPR text does not define the concept of "privacy", but refers to Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002, concerning personal data processing and privacy protection in the electronic communications sector (further – Directive 2002/58/EC)[26]. GDPR uses the concept of "personal data". According to EDPB[27], EDPS[28], and ENISA[29], in the context of projected privacy, the concepts of "personal data" and "privacy" should be considered as synonyms. In addition, EDPB, EDPS, and ENISA guidelines stipulate that for situations of low importance, no distinction should be made between personal data protection and privacy by design and by default.

---

25 Langheinrich, M. Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems: Distributed Systems Group Institute of Information Systems, IFW Swiss Federal Institute of Technology, ETH Zurich 8092 Zurich, Switzerland. https://clck.ru/36h7qq

26 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

27 EDPB is an independent body of the European Union, established and functioning on the basis of the GDPR. EDPB helps to ensure the harmonized application of the GDPR, for which purpose it has a number of powers stipulated by Art. 70 of GDPR. In particular, this body is authorized to issue guidelines, recommendations and best practices for the GDPR application.

28 EDPS is an independent EU body controlling the activities of the national supervisory authorities established in compliance with VGDPR section.

29 The European Union Agency for Cybersecurity (ENISA). https://clck.ru/N598K

However, this common understanding of personal data protection and privacy by design and by default is not accepted in all cases. The published EDPS opinion on Privacy by Design and Default[30] distinguishes between two concepts – privacy by design and data protection by design. The notion of privacy by design is used to refer to a system of technological measures aimed at ensuring privacy, developed in the course of international debates over the last few decades. This notion defines the legal regime of information, which consists in restricting access to it, and means "data protection by technological design" [31] (Zharova, 2020).

"Data protection by design" refers to a preliminary solution on data protection and privacy at the stage of technology design for all user actions[32] (Zharova, 2019).

Discussions over the extent to which these terms differ continue to this day. For example, the developers of explanations on the application of GDPR[33] write that there is still uncertainty about what privacy by design means and how it can be implemented. This problem arises due to the fact that, on the one hand, Directive 95/46/EC[34] is not fully implemented in some member states. On the other hand, according to the privacy by design principle contained in GDPR, data security guidelines require that organizational and technical measures should be adopted as early as at the stage of planning the information system. For example, the GDPR principle of integrity and confidentiality determines the need to protect data against unauthorized access or unlawful processing, as well as against accidental loss, destruction or damage[35]. However, the EU legislation leaves completely open the question of the protective measures taken by the parties responsible. For example, is anonymization of a person's name sufficient to fulfill the legislation requirements?

GDPR proposes using data encryption or anonymization as a possible privacy by design measure. However, this suggestion does not make it clear how this measure would further align with the GDPR's user authentication requirement and the technical implementation of the right to object.

---

30 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. https://clck.ru/36h7v3

31 GDPR Privacy by Design. https://clck.ru/36h7vZ

32 Data protection by design and default. https://goo.su/Hxoh2d

33 GDPR Privacy by Design. https://clck.ru/36h7vZ

34 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://clck.ru/36h7jM

35 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) of 27 April 2016. https://clck.ru/34U2FN

As a result, the authors of the clarifications on GDPR application defined the term "privacy by design" as "data protection through technological design". They believe that "in data processing procedures, data protection is best adhered to when it is already integrated into the technology during its design phase".

Conclusion

The problems of personal data protection, control of users' big data processing principles, and protection of individual's privacy are only getting more acute every year. The need to ensure personal data protection and privacy of an individual as an IT user poses a challenge to the legislator to ensure the openness of the information technology algorithms' logic. To achieve this objective, GDPR stipulates the requirement to implement privacy by design in IT development, which was proposed back in 1995. The requirement to implement the principle of algorithmic transparency in AI systems was proposed much later – in 2019 by Russian lawmakers and in 2018 by foreign lawmakers.

Algorithms of data processing are becoming more and more complex. Hence, legislative proposals to reveal the logic of their functioning, for example, in AI systems, are made more and more often. However, one should understand that such proposals cannot be implemented for all algorithms. It is hardly possible to explain complex mathematical tools in simple words that will be understandable to every common person.

However, this does not mean that there is no solution to this complex technical and legal problem. We believe that the development of information security standards and the inclusion of requirements in legal acts on the IT development in compliance with standardization requirements will minimize the risks associated with the unlawful processing of users' big data and obtaining privacy information.

References

Akter, Sh., Dwivedi, Y. K., Sajib, Sh., Biswas, K., Bandara, R. J., & Michael, K. (2022). Algorithmic bias in machine learning-based marketing models. *Journal of Business Research*, *144*, 201–216. https://doi.org/10.1016/j.jbusres.2022.01.083

Balasubramaniam, N., Kauppinen, M., Rannisto, A., Hiekkanen, K., & Kujala, S. (2023). Transparency and explainability of AI systems: From ethical guidelines to requirements. *Information and Software Technology*, *159*, 107197. https://doi.org/10.1016/j.infsof.2023.107197

Bolton, M., Raven, R., & Mintrom, M. (2021). Can AI transform public decision-making for sustainable development? An exploration of critical earth system governance questions. *Earth System Governance*, *9*, 100116. https://doi.org/10.1016/j.esg.2021.100116

Bujold, A., Parent-Rocheleau, X., & Gaudet, M.-C. (2022). Opacity behind the wheel: The relationship between transparency of algorithmic management, justice perception, and intention to quit among truck drivers. *Computers in Human Behavior Reports*, *8*, 100245. https://doi.org/10.1016/j.chbr.2022.100245

Carlsson, V., & Rönnblom, M. (2022). From politics to ethics: Transformations in EU policies on digital technology. *Technology in Society*, *71*, 102145. https://doi.org/10.1016/j.techsoc.2022.102145

Cui, M., Mariani, M. S., & Medo, M. (2022). Algorithmic bias amplification via temporal effects: The case of PageRank in evolving networks. *Communications in Nonlinear Science and Numerical Simulation*, *104*, 106029. https://doi.org/10.1016/j.cnsns.2021.106029

Custers, B., & Heijne, A.-S. (2022). The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice. *Computer Law & Security Review*, *46*, 105727. https://doi.org/10.1016/j.clsr.2022.105727

de Bruijn, H., Warnier, M., & Janssen, M. (2022). The perils and pitfalls of explainable AI: Strategies for explaining algorithmic decision-making. *Government Information Quarterly*, *39*(2), 101666. https://doi.org/10.1016/j.giq.2021.101666

Feijóo, C., Kwon, Y., Bauer, J. M., Bohlin, E., Howell, B., Jain, R., Potgieter, P., Vu, K., Whalley, J., & Xia, J. (2020). Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. *Telecommunications Policy*, *44*(6), 101988. https://doi.org/10.1016/j.telpol.2020.101988

Gordon, G., Rieder, B., & Sileno, G. (2022). On mapping values in AI Governance. *Computer Law & Security Review*, *46*, 105712. https://doi.org/10.1016/j.clsr.2022.105712

Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. *Computer Law & Security Review*, *45*, 105681. https://doi.org/10.1016/j.clsr.2022.105681

Gulemin, A. (2022). Limits of big data processing for the purposes of obtaining information about a person: a legal aspect. In Elektronnoe prilozhenie k "Rossiiskomu yuridicheskomu zhurnalu", 6, 52–57. (In Russ.). http://doi.org/10.34076/22196838_2022_6_52

Kempeneer, Sh. (2021). A big data state of mind: Epistemological challenges to accountability and transparency in data-driven regulation. *Government Information Quarterly*, *38*(3), 101578. https://doi.org/10.1016/j.giq.2021.101578

Kempeneer, Sh., Pirannejad, A., & Wolswinkel, J. (2023). Open government data from a legal perspective: An AI-driven systematic literature review. *Government Information Quarterly*, 101823. https://doi.org/10.1016/j.giq.2023.101823

Kuteynikov, D. L., Izhaev, O. A., Zenin, S. S., & Lebedev, V. A. (2020). Algorithmic transparency and accountability: legal approaches to solving the "black box" problem. *Lex russica*, *73*(6), 139–148. (In Russ.). https://doi.org/10.17803/1729-5920.2020.163.6.139-148

Lang, H., & Shan, C. (2000). Bias phenomenon and compensation in multiple target tracking algorithms. *Mathematical and Computer Modelling*, *31*(8–9), 147–165. https://doi.org/10.1016/S0895-7177(00)00063-7

Leerssen, P. (2023). An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review*, *48*, 105790. https://doi.org/10.1016/j.clsr.2023.105790

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Li, Z. (2022). Affinity-based algorithmic pricing: A dilemma for EU data protection law. *Computer Law & Security Review*, *46*, 105705. https://doi.org/10.1016/j.clsr.2022.105705

Malyshkin, A. V. (2019). Integration of artificial intelligence into public life: some ethical and legal problems. *Vestnik of Saint Petersburg University. Law*, *10*(3), 444–460. (In Russ.). https://doi.org/10.21638/spbu14.2019.303

Matheus, R., Janssen, M., & Janowski, T. (2021). Design principles for creating digital transparency in government. *Government Information Quarterly*, *38*(1), 101550. https://doi.org/10.1016/j.giq.2020.101550

Mourby, M., Ó Cathaoir, K., & Bjerre Collin, C. (2021). Transparency of machine-learning in healthcare: The GDPR & European health law. *Computer Law & Security Review*, *43*, 105611. https://doi.org/10.1016/j.clsr.2021.105611

Ostroumov, N. N. (2015). Legal regime of international air transportation. Moscow: Statut. (In Russ.).

Qiaochu, W., Yan, H., Stefanus, J., & Param Vir, S. (2020, July 15). *Algorithmic Transparency with Strategic Users*. http://dx.doi.org/10.2139/ssrn.3652656

Robinson, S. C. (2020). Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI). *Technology in Society*, *63*, 101421. https://doi.org/10.1016/j.techsoc.2020.101421

Stahl, B. C., Rodrigues, R., Santiago, N., & Macnish, K. (2022). A European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values. *Computer Law & Security Review*, *45*, 105661. https://doi.org/10.1016/j.clsr.2022.105661

Stefik, M. (1996). Letting loose the light: Igniting commerce in electronic publication. In M. Stefik (Ed.), *Internet dreams: Archetypes, myths, and metaphors* (pp. 219–253). Cambridge, MA: MIT Press.

Stöger, K., Schneeberger, D., Kieseberg, P., & Holzinger, A. (2021). Legal aspects of data cleansing in medical AI. *Computer Law & Security Review*, *42*, 105587. https://doi.org/10.1016/j.clsr.2021.105587

Su, Zh., Bentley, B. L., McDonnell, D., Cheshmehzangi, A., Ahmad, J., Šegalo, S., Pereira da Veiga, C., & Xiang, Yu-Tao. (2023). China's algorithmic regulations: Public-facing communication is needed. *Health Policy and Technology*, *12*(1), 100719. https://doi.org/10.1016/j.hlpt.2022.100719

Talapina, E. V. (2020). Algorithms and artificial intelligence in the human rights context. *Journal of Russian Law*, *10*, 25–39. (In Russ.). https://doi.org/10.12737/jrl.2020.118.

Varsha, P. S. (2023). How can we manage biases in artificial intelligence systems – A systematic literature review. *International Journal of Information Management Data Insights*, *3*(1), 100165. https://doi.org/10.1016/j.jjimei.2023.100165

Wang, H. (2022). Transparency as Manipulation? Uncovering the Disciplinary Power of Algorithmic Transparency. *Philosophy & Technology*, *35*, 69. https://doi.org/10.1007/s13347-022-00564-w

Willems, J., Schmidthuber, L., Vogel, D., Ebinger, F., & Vanderelst, D. (2022). Ethics of robotized public services: The role of robot design and its actions. *Government Information Quarterly*, *39*(2), 101683. https://doi.org/10.1016/j.giq.2022.101683

Xu, J., Xiao, Yu., Wang, W. Hu., Ning, Yu., Shenkman, E. A., Bian, J., & Wang, F. (2022). Algorithmic fairness in computational medicine. *eBioMedicine*, *84*, 104250. https://doi.org/10.1016/j.ebiom.2022.104250

Zharova, A. (2019). Ensuring the information security of information communication technology users in Russia. *International Journal of Cyber Criminology*, *13*(2), 255–269. DOI: https://doi.org/10.5281/zenodo.3698141

Zharova, A. (2020). The protect mobile user data in Russia. *International Journal of Electrical and Computer Engineering*, *10*(3), 3184–3192. https://doi.org/10.11591/ijece.v10i3.pp3184-3192

Zhu, H., Sallnäs Pysander, E.-L., & Söderberg, I.-L. (2023). Not transparent and incomprehensible: A qualitative user study of an AI-empowered financial advisory system. *Data and Information Management*, 100041. https://doi.org/10.1016/j.dim.2023.100041

Author information

Anna K. Zharova – Dr. Sci. (Law), Associate Professor, Senior Researcher, Institute of State and Law of the Russian Academy of Sciences
Address: 10 Znamenka Str., 420100 Moscow, Russian Federation
E-mail: anna_jarova@mail.ru
ORCID ID: https://orcid.org/0000-0002-2981-3369
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56964137900
WoS Researcher ID: https://www.webofscience.com/wos/author/record/H-4012-2015
Google Scholar ID: https://scholar.google.com/citations?user=g8ij3BsAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=151076

Conflict of interest

The author is an Editor-in-Chief of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research was not sponsored.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – May 22, 2023
Date of approval – August 21, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:346.1:006.44:004.8
EDN: https://elibrary.ru/oppobg
DOI: https://doi.org/10.21202/jdtl.2023.42

Достижение алгоритмической прозрачности и управление рисками информационной безопасности при принятии решений без вмешательства человека: правовые подходы

Анна Константиновна Жарова

Институт государства и права Российской академии наук
г. Москва, Российская Федерация

Ключевые слова

GDPR,
алгоритмическая прозрачность,
защита данных,
информационная безопасность,
информационные технологии,
искусственный интеллект,
конфиденциальность,
персональные данные,
право,
цифровые технологии

Аннотация

Цель: сравнение современных подходов в праве к использованию в процессе принятия решений программных кодов и алгоритмов, отвечающих принципам прозрачности и открытости, а также возрастающим требованиям к обеспечению безопасности персональных и иных больших данных, полученных и обработанных алгоритмическим путем.

Методы: основными методами исследования принципа прозрачности алгоритмизированного принятия решений являлись формально-юридический и сравнительный анализ правовых актов и международных стандартов информационной безопасности, содержащихся в них принципов и правовых конструкций.

Результаты: определено, что развитие области стандартизации информационной безопасности, включение в правовые акты требований о разработке информационных технологий, соответствующих принципам прозрачности и открытости применяемых алгоритмов, позволит минимизировать риски, связанные с неправомерными обработкой больших пользовательских данных и получением информации об их частной жизни; выявлены связанные с реализацией алгоритмической прозрачности предложения в области правового регулирования обработки данных; сформулированы рекомендации, с опорой на которые законодатель может решать задачу обеспечения открытости логики работы алгоритмов информационных технологий с учетом современных стандартов информационной безопасности.

Научная новизна: состоит в обосновании новых тенденций и формируемых в соответствии с ними правовых подходов, позволяющих раскрыть логику обработки данных цифровыми и информационными технологиями, на основе характеристики общеевропейских стандартов концепции конфиденциальности при проектировании новых цифровых и информационных технологий принятия решений и защиты данных, новых правовых требований, предъявляемых к системам искусственного интеллекта, включая требование об обеспечении алгоритмической прозрачности, критериев обработки персональных данных, а также больших пользовательских данных. При этом защита данных рассматривается как система правовых, технических и организационных принципов, направленная на обеспечение конфиденциальности персональных данных.

Практическая значимость: обусловлена необходимостью изучения передового отечественного и международного опыта защиты частной жизни пользователей цифровых и информационных технологий, а также законодательного обеспечения требований об использовании алгоритмов, отвечающих принципам прозрачности и открытости обработки персональных данных с учетом необходимости обеспечения конфиденциальности на всех этапах жизненного цикла их обработки, что позволит обеспечить непрерывность управления безопасностью.

Для цитирования

Жарова, А. К. (2023). Достижение алгоритмической прозрачности и управление рисками информационной безопасности при принятии решений без вмешательства человека: правовые подходы. *Journal of Digital Technologies and Law*, *1*(4), 973–993. https://doi.org/10.21202/jdtl.2023.42

Список литературы

Гулемин, А. Н. (2022). Пределы обработки больших объемов данных для целей получения информации о человеке: правовой аспект. *Электронное приложение к Российскому юридическому журналу*, *6*, 52–57. http://doi.org/10.34076/22196838_2022_6_52

Кутейников, Д. Л., Ижаев, О. А., Зенин, С. С., Лебедев, В. А. (2020). Алгоритмическая прозрачность и подотчетность: правовые подходы к разрешению проблемы «черного ящика». *Lex russica (Русский закон)*, *73*(6), 146. https://doi.org/10.17803/1729-5920.2020.163.6.139-148

Малышкин, А. В. (2019). Интегрирование искусственного интеллекта в общественную жизнь: некоторые этические и правовые проблемы. Вестник Санкт-Петербургского университета. *Право*, *10*(3), 444–460. https://doi.org/10.21638/spbu14.2019.303

Остроумов, Н. Н. (2015). *Правовой режим международных воздушных перевозок*. Москва: Статут. https://elibrary.ru/ulcfpl

Талапина, Э. В. (2020). Алгоритмы и искусственный интеллект сквозь призму прав человека. *Журнал российского права*, *10*, 25–39. https://doi.org/10.12737/jrl.2020.118

Akter, Sh., Dwivedi, Y. K., Sajib, Sh., Biswas, K., Bandara, R. J., & Michael, K. (2022). Algorithmic bias in machine learning-based marketing models. *Journal of Business Research*, *144*, 201–216. https://doi.org/10.1016/j.jbusres.2022.01.083

Balasubramaniam, N., Kauppinen, M., Rannisto, A., Hiekkanen, K., & Kujala, S. (2023). Transparency and explainability of AI systems: From ethical guidelines to requirements. *Information and Software Technology*, *159*, 107197. https://doi.org/10.1016/j.infsof.2023.107197

Bolton, M., Raven, R., & Mintrom, M. (2021). Can AI transform public decision-making for sustainable development?

An exploration of critical earth system governance questions. *Earth System Governance*, *9*, 100116. https://doi.org/10.1016/j.esg.2021.100116

Bujold, A., Parent-Rocheleau, X., & Gaudet, M.-C. (2022). Opacity behind the wheel: The relationship between transparency of algorithmic management, justice perception, and intention to quit among truck drivers. *Computers in Human Behavior Reports*, *8*, 100245. https://doi.org/10.1016/j.chbr.2022.100245

Carlsson, V., & Rönnblom, M. (2022). From politics to ethics: Transformations in EU policies on digital technology. *Technology in Society*, *71*, 102145. https://doi.org/10.1016/j.techsoc.2022.102145

Cui, M., Mariani, M. S., & Medo, M. (2022). Algorithmic bias amplification via temporal effects: The case of PageRank in evolving networks. *Communications in Nonlinear Science and Numerical Simulation*, *104*, 106029. https://doi.org/10.1016/j.cnsns.2021.106029

Custers, B., & Heijne, A.-S. (2022). The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice. *Computer Law & Security Review*, *46*, 105727. https://doi.org/10.1016/j.clsr.2022.105727

de Bruijn, H., Warnier, M., & Janssen, M. (2022). The perils and pitfalls of explainable AI: Strategies for explaining algorithmic decision-making. *Government Information Quarterly*, *39*(2), 101666. https://doi.org/10.1016/j.giq.2021.101666

Feijóo, C., Kwon, Y., Bauer, J. M., Bohlin, E., Howell, B., Jain, R., Potgieter, P., Vu, K., Whalley, J., & Xia, J. (2020). Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. *Telecommunications Policy*, *44*(6), 101988. https://doi.org/10.1016/j.telpol.2020.101988

Gordon, G., Rieder, B., & Sileno, G. (2022). On mapping values in AI Governance. *Computer Law & Security Review*, *46*, 105712. https://doi.org/10.1016/j.clsr.2022.105712

Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. *Computer Law & Security Review*, *45*, 105681. https://doi.org/10.1016/j.clsr.2022.105681

Kempeneer, Sh. (2021). A big data state of mind: Epistemological challenges to accountability and transparency in data-driven regulation. *Government Information Quarterly*, *38*(3), 101578. https://doi.org/10.1016/j.giq.2021.101578

Kempeneer, Sh., Pirannejad, A., & Wolswinkel, J. (2023). Open government data from a legal perspective: An AI-driven systematic literature review. *Government Information Quarterly*, 101823. https://doi.org/10.1016/j.giq.2023.101823

Lang, H., & Shan, C. (2000). Bias phenomenon and compensation in multiple target tracking algorithms. *Mathematical and Computer Modelling*, *31*(8–9), 147–165. https://doi.org/10.1016/S0895-7177(00)00063-7

Leerssen, P. (2023). An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review*, *48*, 105790. https://doi.org/10.1016/j.clsr.2023.105790

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Li, Z. (2022). Affinity-based algorithmic pricing: A dilemma for EU data protection law. *Computer Law & Security Review*, *46*, 105705. https://doi.org/10.1016/j.clsr.2022.105705

Matheus, R., Janssen, M., & Janowski, T. (2021). Design principles for creating digital transparency in government. *Government Information Quarterly*, *38*(1), 101550. https://doi.org/10.1016/j.giq.2020.101550

Mourby, M., Ó Cathaoir, K., & Bjerre Collin, C. (2021). Transparency of machine-learning in healthcare: The GDPR & European health law. *Computer Law & Security Review*, *43*, 105611. https://doi.org/10.1016/j.clsr.2021.105611

Qiaochu, W., Yan, H., Stefanus, J., & Param Vir, S. (2020, July 15). *Algorithmic Transparency with Strategic Users*. http://dx.doi.org/10.2139/ssrn.3652656

Robinson, S. C. (2020). Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI). *Technology in Society*, *63*, 101421. https://doi.org/10.1016/j.techsoc.2020.101421

Stahl, B. C., Rodrigues, R., Santiago, N., & Macnish, K. (2022). A European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values. *Computer Law & Security Review*, *45*, 105661. https://doi.org/10.1016/j.clsr.2022.105661

Stefik, M. (1996). Letting loose the light: Igniting commerce in electronic publication. In M. Stefik (Ed.), *Internet dreams: Archetypes, myths, and metaphors* (pp. 219–253). Cambridge, MA: MIT Press.

Stöger, K., Schneeberger, D., Kieseberg, P., & Holzinger, A. (2021). Legal aspects of data cleansing in medical AI. *Computer Law & Security Review*, *42*, 105587. https://doi.org/10.1016/j.clsr.2021.105587

Su, Zh., Bentley, B. L., McDonnell, D., Cheshmehzangi, A., Ahmad, J., Šegalo, S., Pereira da Veiga, C., & Xiang, Yu-Tao. (2023). China's algorithmic regulations: Public-facing communication is needed. *Health Policy and*

Technology, *12*(1), 100719. https://doi.org/10.1016/j.hlpt.2022.100719

Varsha, P. S. (2023). How can we manage biases in artificial intelligence systems – A systematic literature review. *International Journal of Information Management Data Insights*, *3*(1), 100165. https://doi.org/10.1016/j.jjimei.2023.100165

Wang, H. (2022). Transparency as Manipulation? Uncovering the Disciplinary Power of Algorithmic Transparency. *Philosophy & Technology*, *35*, 69. https://doi.org/10.1007/s13347-022-00564-w

Willems, J., Schmidthuber, L., Vogel, D., Ebinger, F., & Vanderelst, D. (2022). Ethics of robotized public services: The role of robot design and its actions. *Government Information Quarterly*, *39*(2), 101683. https://doi.org/10.1016/j.giq.2022.101683

Xu, J., Xiao, Yu., Wang, W. Hu., Ning, Yu., Shenkman, E. A., Bian, J., & Wang, F. (2022). Algorithmic fairness in computational medicine. *eBioMedicine*, *84*, 104250. https://doi.org/10.1016/j.ebiom.2022.104250

Zharova, A. (2019). Ensuring the information security of information communication technology users in Russia. *International Journal of Cyber Criminology*, *13*(2), 255–269. EDN: https://elibrary.ru/ltmesv. DOI: https://doi.org/10.5281/zenodo.3698141

Zharova, A. (2020). The protect mobile user data in Russia. *International Journal of Electrical and Computer Engineering*, *10*(3), 3184–3192. EDN: https://www.elibrary.ru/juzboh. DOI: https://doi.org/10.11591/ijece.v10i3.pp3184-3192

Zhu, H., Sallnäs Pysander, E.-L., & Söderberg, I.-L. (2023). Not transparent and incomprehensible: A qualitative user study of an AI-empowered financial advisory system. *Data and Information Management*, 100041. https://doi.org/10.1016/j.dim.2023.100041

Сведения об авторе

Жарова Анна Константиновна – доктор юридических наук, доцент, старший научный сотрудник, Институт государства и права Российской академии наук
Адрес: 420100, Российская Федерация, г. Москва, ул. Знаменка, 10
E-mail: anna_jarova@mail.ru
ORCID ID: https://orcid.org/0000-0002-2981-3369
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56964137900
WoS Researcher ID: https://www.webofscience.com/wos/author/record/H-4012-2015
Google Scholar ID: https://scholar.google.com/citations?user=g8ij3BsAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=151076

Конфликт интересов

Автор является главным редактором журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.61 / Правовое регулирование информационной безопасности
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 22 мая 2023 г.
Дата одобрения после рецензирования – 21 августа 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.43

Employing the Responsibility to Protect (R2P) to Impose Universal Jurisdiction Regarding Cyber-Terrorism

Yassin Abdalla Abdelkarim

Luxor Elementary Court
Sohag, Egypt

Keywords

crimes against humanity,
cybersecurity,
cyberspace,
cyberterrorism,
digital technologies,
human rights,
international private law,
international public law,
jurisdiction,
law

Abstract

Objective: the development of wireless technologies and digital infrastructure has radically changed the human habitat, giving rise to a new type of space – a cyberspace. The uniqueness and peculiarities of this environment, including anonymity, boundlessness and problems related to the determination and establishment of jurisdiction, have become a breeding ground for the emergence of a new global threat – cyberterrorism. The latter is characterized by a high level of latency, low detection rate and incomparably greater danger than "real world" crimes. Countering new forms of crime has required the development of universal tools that overcome the limitations of traditional jurisdiction and allow states to prosecute terrorists in cyberspace. Identifying the relevant tools and identifying the political-legal obstacles to their implementation is the objective of this study.

Methods: to achieve the set goal the formal-legal method was used to analyze legal sources, including judicial practice, national legislation, and international acts. The doctrinal approach was also used, which allowed, on the basis of scientific works and theoretical constructions, explaining the complexity of the modern phenomena and predicting their future development. This said, the main focus is on criminals to prove their antagonism with humanity in accordance with theoretical views. Finally, the study analyzes the theories of universal and traditional jurisdiction and how they are applied to prosecute terrorists.

Results: the paper provides a critical analysis, reviewing and adapting the concept of jurisdiction as applied to a global, borderless and decentralized digital environment (cyberspace) and to the struggle against new forms of terrorism (cyberterrorism). Various jurisdictional models applicable in cyberspace are presented. The author bridges the gap between the main branches of law: international private law and public law by linking, in relation to cyberterrorism, the two theories: the "responsibility to protect" (R2P) theory and the application of universal jurisdiction. The trends of universal jurisdiction development are revealed.

Scientific novelty: the study develops the accumulated scientific knowledge while justifying the introduction of foreign jurisdiction in a state territory to prosecute cyberterrorists. It also establishes a link between the theory of universal jurisdiction in private international law and the "responsibility to protect" (R2P) theory in public international law, recognizing the latter as a relevant basis for the introduction of universal jurisdiction over cyberterrorism. Such traditional concepts as sovereignty and jurisdictional independence are reviewed. The gap related to the consideration of cyberterrorism as a crime against humanity in international law is bridged.

Practical significance: the implementation of the proposed conclusions will contribute to the strengthening of international prosecution of cyberterrorism and harmonize the international and national legal tools to struggle against this crime.

For citation

Abdelkarim, Y. A. (2023). Employing the Responsibility to Protect (R2P) to Impose Universal Jurisdiction Regarding Cyber-Terrorism. *Journal of Digital Technologies and Law, 1*(4), 994–1022. https://doi.org/10.21202/jdtl.2023.43

Contents

Introduction

International scholars acknowledge the duties entitled in the "Responsibility to Protect" theory to protect human rights. Also, they admit the global nature of cyber-terrorism destruction. Consequently, this theory is the appropriate reasoning for imposing universal jurisdiction regarding cyber-terrorism. The research introduces the "Responsibility to Protect" (further – R2P) theory as the pillar to impose universal jurisdiction regarding cyber-terrorism. It establishes a link between the two international law theories: Universal Jurisdiction from international private law and the Responsibility to Protect from international public law.

The research contributes to knowledge by providing the international community with the legal justification to impose foreign jurisdictions within a state territory to prosecute cyber-terrorists. It establishes a link between the universal jurisdiction theory in international private law and the responsibility to protect in international public law. Therefore, it bridges a gap between these major branches of international law. Besides, it recontextualizes traditional concepts, e.g., sovereignty and jurisdictional independence, to achieve prior humanitarian aims. Furthermore, it bridges the gap in knowledge by linking cyber-terrorism to the established concept of crimes against humanity in international law; it proves the applicability of the latter elements to cyber-terrorism as an international illegal activity. Thus, the R2P theory could be utilized to impose universal jurisdiction regarding it just as CAH.

The research analyzes the structure of cyber-terrorism and explores its camouflaged elements under cyberspace's ambiguity. The limitlessness of the latter requires developing a tool that transcends the odds of traditional jurisdictions. This tool is universal jurisdiction; it permits states to prosecute terrorists in cyberspace, regardless of their location. Yet, its application faces obstacles, legal and political. Therefore, a theory that includes obligatory concepts would be an effective tool to support it.

The research enhances international prosecution of cyber-terrorism as it justifies utilizing global legal toolkits against it. It proves that cyber-terrorism is a crime against humanity that triggers international intervention under the R2P theory, which it presents as a regulative legal norm. So, it manifests global solidarity to prevent those serious

crimes under the UN Charter rules by harmonizing international and domestic legal toolkits concerning this crime. Consequently, international jurisprudence encircles cyber-terrorism and eliminates its evil in cyberspace.

Regarding the methodology, the research adopts a theoretical approach to achieve its objectives. It is established on a doctrinal method to examine legal sources to analyze the legal prepositions found in primary and secondary legal resources. It includes case laws, domestic legislation, and international instruments. The analysis depends on logical reasoning. This approach analyses the norms that the legal materials included to elaborate the legal understanding of the research question. Besides, argumentized reviews of case laws and primary law resources contribute to extracting the relevant approaches.

The research reviews the relevant scholarships to disclose the gap in knowledge that the research bridges. It discusses the contextualization of the R2P theory, emphasizing its purpose, which is to defend humanity against atrocities. Then, the research explores the concept of cyber-terrorism to extract its theory from academics. Mainly, it focuses on the perpetrator's side of this activity to prove its antagonism to humanity according to the theorists' views. At last, the research refutes the outstanding literature on universal jurisdiction theory and how jurisdictions adopt it to prosecute terrorists.

Besides, it analyzes international and domestic law sources to study how they handled universal jurisdiction as they prosecute cyber-terrorists. Also, it reviews the relevant literature to set out the trending attitudes about universal jurisdiction.

1. The Preventive Nature of the R2P Regarding Crimes Against Humanity (CAH)

International law includes obligations on states to protect humanity against atrocities. These obligations are binding according to their legal roots. The International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social, and Cultural Rights (ICSECR) mention fundamental human rights as the subject of protection. Beforehand, the 1948 Genocide Convention imposed a duty on states to prevent genocide crimes[1]. Also, the UN Charter adopts these duties to defend humanity by securing international peace. Indeed, the evolution of the UN doctrine tended to adopt this responsibility as protection from CAH[2]. It is clear in the 2005 World Summit report that a global theory of international community responsibility should be enacted to achieve the UN aims. These legal instruments include the threshold to trigger the state's obligations. The binding force of these obligations reflects their enforceability in the global legal system and the nations determination to protect humanity. So, the concept of responsibility to protect is rooted in international law.

1 The 1948 Convention on the Prevention and Punishment of the Crime of Genocide, Arts 3, 6 and 8.

2 The UN General Assembly. Resolution Adopted by the General Assembly: 60/1 (UN, 2005), para. 139 and the Resolution A/75/277 (UN 2021), para. 6.

1.1. The Universalization of the R2P to Prevent CAH

This doctrine affirms the R2P as an international legal norm that aims to prevent inhumane atrocities. It was mentioned in the UN Security Council resolutions (UNSC) to justify intervention in preventing CAH[3]. This attitude shifts the R2P from an innovative idea to an acknowledged legal principle in international law. Then, it introduces a systematic legal foundation to intervene in preventing CAH (Cantini & Zavialov, 2018). CAH imply the accountability of the international community to act, regardless of sovereignty considerations. Thus, the R2P implies facilitating the CAH prevention measures undertaken by the international community or a foreign jurisdiction (Cantini & Zavialov, 2018).

Royer claims that states' political will and the traditional understanding of their sovereignty hinder the international community intervention to prevent CAH (Royer, 2021). So, he emphasizes that states should integrate the R2P into the interpretation of their national interests regarding CAH (Royer, 2021). He argues that the R2P does not manifest a valuable reference for state politics that they might oppose its application. This fact implies reconceptualizing the international community's endeavors to combat evil in a political framework. Yet, while the R2P represents a moral norm, doctrine should review it as a preventive procedure to protect humanity (Royer, 2021). This integration supports the R2P in international politics as it eliminates extremist patriotic odds that oppose foreign intervention. Royer's reframing of the R2P underlines the severity of CAH as a common evil that requires global collaboration to suppress it.

Furthermore, Watt argues that the R2P should be constitutionalized in international law under the authority of the UN institutions (Wyatt, 2019). He claims that the R2P is an extension of UN humanity protection since it imposes a collective responsibility on member states to prevent CAH (Wyatt, 2019). In addition, it would overcome the strict Westphalian view of state sovereignty[4], pointing out it from the responsibility aspect. So, a moral relationship is established between it and cosmopolitan human protection. Moreover, he considers the UN organs the effective bodies to enforce the R2P legal order. So, they should surveil the application of the R2P. This constitutional order guarantees the effective integration of the R2P duties into a firm establishment of international commitments. It manifests a global level of the solidarity obligation included in the UN Charter. It provides international diplomacy and doctrine with a harmonized concept of solidarity to maintain peace and security[5]. He seeks, through

3 Resolutions 1674 (2006), 63/308 (2009)68 and 1894 (2009).

4 'Supreme authority within a territory', ibid, p. 99.

5 Ibid, p. 156.

his interpretation, to consolidate the R2P in international law and diplomacy. Trying to impose the constitutional nature of the R2P on states requires their clear consent of them as it might contradict their interpretation of sovereignty. Besides, the mentioned harmonization implies unifying the views of states on their responsibilities to prevent CAH from considering the solidarity obligation of the Charter. In practice, politics frustrates the R2P efforts by considering it a Western imperialism that should be patriotically resisted. Despite that the NATO intervention in Libya was approved by the UNSC under the R2P norms[6], it was criticized as it violated state sovereignty and led to political chaos therein. It might be overseen exploitation of international justice for political aims. To overcome this odd, international jurisprudence should contextualize the R2P legally according to each case separately to ensure its impartiality.

CAH by a third party, e.g., terrorists, on a group of local population trigger international responsibility to intervene to prevent them if the host state did not respond (Soler, 2019). External intervention could utilize foreign jurisdictional tools to prosecute these crimes. This responsibility consists of both state and international community duties to prevent severe atrocities which violate fundamental human rights (Park & Switzer, 2020) through the transnationalism of legal procedures[7]. Therefore, the R2P aims are guaranteed by this intervention as its humanitarian aspects overwhelm sovereignty claims. This duty of the international community is sustained by the non-fulfillment of the host state of its responsibility to protect fundamental human rights. Also, CAH must not exploit state sovereignty as a shield to avoid prosecution (Soler, 2019). Moreover, international law permits humanitarian intervention to prevent human rights violations even by use of force, though its rare cases (Azubuike, 2023). A fortiori, judicial intervention is an appropriate solution to defend these rights. These rights are rooted in international law that grants them continuous protection.

Remarkably, the R2P norms could be utilized in cyberspace to suppress terrorist activities by promoting the collaboration of internet giants and national bodies to enforce responsible measures to achieve this aim (Park & Switzer, 2020). This supports the R2P's existence in cyberspace since it presents this theory as a shield against cyber-terrorism.

6 The United Nations Security Council S/RES/1973 (2011), para. 4.

7 Kosiba, K. (2018). Is R2P the Remedy for Illegal Deforestation? A Case Study Based on the Systematic Human Rights Violations in Peru. Master of Arts Dissertation submitted to the Brussels School of International Law. University of Kent. https://clck.ru/36ksvy

1.2. International Jurisprudence Utilization of the R2P

The International Court of Justice establishes the R2P as the collective obligation to maintain international peace and security[8]. So, states must utilize the reasonably available methods to achieve this purpose. The R2P represents, at its core, a due diligence obligation since states are not obliged to succeed in preventing those crimes completely[9]. This jurisprudence proves the flexibility of the R2P in international law that makes it suitable reasoning for applying universal toolkits, i.e., universal jurisdiction, regarding CAH.

Establishing accountability for CAH enhances the ICC agenda to ensure effective human protection (Bellamy, 2018). At this point, the R2P accords with the Rome Statute objectives as it could be employed to provide a legal pillar of the ICC tools. The R2P utilizes non-military preventive measures of the ICC to suppress CAH under Article 7 of the Statute (Holvoet & Mema, 2015). Indeed, the ICC proves efficient to achieve this purpose because of its preventive and permanent characteristics (Holvoet & Mema, 2015). Thus, this integrated establishment of the ICC tools and the R2P constitutes a shield that protects humanity against CAH.

This humanitarian end justifies the utilization of these tools even for non-party states, particularly under the approval of the R2P in the UNSC resolutions. Yet, the R2P, to be effective, should instrumentalize diplomatic and humanitarian mechanisms (Bellamy, 2018). This approach includes employing legal toolkits from foreign jurisdictions. For instance, the ICC imposed its jurisdiction in Kenya and issued an ultimatum to the government about establishing an ad hoc court for post-election violence (Bellamy, 2018). The ICC's legal efforts, in this case, represented the R2P theory as it tended to protect the local population against violence. Bellamy concludes that both the R2P and the ICC system are integrated humanitarian establishments to prevent CAH. Despite the skeptics, the implementation of non-military measures under the R2P introduces them as alternatives to military operations (Fehl, 2015). They are intermediate stages before waging wars. Thus, their prominence in the R2P theory is unneglectable, which endorses the judicial intervention measures to prevent international crimes.

Notwithstanding the ICC and the R2P's mutual role in preventing CAH, utilizing the court's universal toolkits should be subordinate to the Statute's aims (Holvoet & Mema, 2015). This restriction guarantees the effectiveness and trueness of the ICC measures regarding CAH since it creates judicial surveillance on ICC practices. This mechanism, consequently, enhances the trustworthiness of the ICC's role against CAH and limits the

[8] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (BiH v Serbia and Montenegro), 26 February 2007, ICJ Reports 2007 p. 43, para 166.

[9] Ibid.

perpetrators' impunity. As Ercan elaborates, the R2P toolkit defends international justice and security because it endorses international intervention to guarantee global compliance with international law (Ercan, 2022).

To sum up, scholarships and jurisprudence agree on establishing the R2P on the need to maintain peace and security. In this view, it introduces a legal norm that justifies jurisdictional intervention concerning serious CAH. Thus, it is an appropriate justification to employ foreign legal rules, particularly universal jurisdiction, within the state of crime location. Hence, it overcomes sovereignty claims that might hinder defending human security and encourage the international community to fulfill their duties to protect humanity.

2. The Legal Foundations to Profile Cyber-Terrorism as "Other Inhumane Acts" under the Rome Statute

It is non-debatable that cyberspace establishes international connections between separated nations. Because of its technical nature, terrorists exploit its advantageous facilities to achieve their aims. It enables them to avoid prosecution measures of national law enforcement authorities. Therefore, they operate globally, threatening world peace. Cyber-terrorism is an established inhumane activity that imposes international legal efforts to frustrate it.

Maintaining international peace and security is a leading purpose of international legal bodies, i.e., the International Criminal Court. It is the competent authority to prosecute global perpetrators because of its international legal capabilities. Yet, the Rome Statute, which organizes it, mentions the acts of the court's jurisdiction exclusively. It does not mention cyber-terrorism among them. Though, it notes that the court jurisdiction extends to non-mentioned inhumane acts under certain conditions[10].

Therefore, the article introduces the legal pillars to consider cyber-terrorism a crime against humanity under the Rome Statute of the ICC. The deal of evil of this activity suffices to profile it with this classification, which drops if under the ICC jurisdiction. The article analyzes cyber-terrorism and reviews the literature on it to extract its core elements. Then, it reconceptualizes international law doctrine on crimes against humanity to prove the applicability of this concept to cyber-terrorism. This objective contributes to knowledge by providing the legal basis to extend the ICC's jurisdiction to prosecute cyber-terrorists. This global criminal activity requires a global legal mechanism to hinder it. Consequently, the international community cuts off cyber-terrorism, enhancing world peace and security.

[10] The Rome Statute of the International Criminal Court (2002), Article 7 (1) (k), A/CONF.183/9.

2.1. An Analysis of Cyber-terrorism

In the era of information, terrorism has penetrated cyberspace, shaping a modern threat to humanity. Cyber-terrorism is the utilization of the Internet to target a group with terror for political or radical aims (Broeders et al., 2021). It is a distinctive sort of terrorism that should be analyzed from a broad aspect. Cyber-terrorism exploits the uncontrolled outreach of the internet that strengthens the ties between nations. The French national defense glossary adopts the "risk of terrorism" factor concerning illegal cyber activities (Delerue et al., 2019) to characterize cyber-terrorism. Thus, terrorist groups can act transnationally, transcending geographic proximity (Albahar, 2019). This feature drives scholars to study cyber-terrorism from an international aspect. Accordingly, Alexandra Perloff-Giles profiles cyber-terrorists as "an enemy to mankind" (Perloff-Giles, 2018). She justifies that by the common features between cyber-terrorism and piracy crimes since they both threaten international trade interests. She emphasizes that these attacks jeopardize critical cyber services for a considerable while, which points out the severity of this activity. In addition, she argues that transnational cyber offenses have three concretes:

– the intentional act that harms innocents, as it should be a deliberate attack on national infrastructure or governmental, or private, computer systems. This applies to both governmental and non-state actors. The latter include cyber-terrorists.

– it must occur in cyberspace, exploiting its ambiguity to gain anonymity and advantageous low-cost attacks,

– and it is transnational modus operandi because the perpetrators operate beyond national borders. Perloff-Giles indicates that the malware codes they send need no passport to cross borders. Also, the impacts of their offenses affect several jurisdictions (Perloff-Giles, 2018).

Moreover, Perloff-Giles claims that cyberattacks, regardless of the perpetrators, constitute an illegal use of force, triggering the right to self-defense under Article 51 of the UN Charter. This leads to the application of international humanitarian law, which is a suitable legal set to organize the consequences of cyber conflicts. Yet, she determines the following provisions to apply it:

– the severity and scale of the attacks. Though, she requires a threshold to qualify them for the description "an armed attack",

– and identifying the perpetrators to establish their responsibility. Still, she admits the difficulty to determine this attribution regarding cyber offenses (Perloff-Giles, 2018).

Therefore, Perloff-Giles points out the prominence of cyber offenses as a unique pattern of aggression by terrorists. This activity elevates to application of International Humanitarian Law (IHL) the same as conventional armed conflicts. Thus, this applicability denotes that cyber-terrorism is a severe threat to humanity that requires the utilization of international doctrine efforts to crystallize its dimensions and propose the appropriate legal sets to combat it.

Likewise, in her book "Defining International Terrorism", Stella Margariti claims that terrorism threatens the universal interests of the international community by degrading fundamental human rights concerning international security and peace (Margariti, 2017). She sheds light on the international pillar of terrorism as she claims that its impacts transcend national borders to the international community (Margariti, 2017). Then, since cyberspace exceeds states' geographic borders, the international theme overwhelms its nature. This theme implies the surpassing of criminal acts in cyberspace beyond domestic limits. Consequently, cyber-terrorism generates inevitable impacts on international security.

Because of its limitlessness, terrorist groups utilize cyberspace to achieve their purposes. It is recorded that militants like ISIS exploit social media websites to spread their terror by broadcasting their video content. Besides, they use these websites as recruitment platforms. Thus, they can operate globally beyond geographic borders (Awan, 2017). This utility grants terrorists an advantage over law enforcement and security measures. Also, it emphasizes the need to study cyber-terrorism as an independent criminal activity that combines terror and technology.

Notably, Victoria Correia defines cyber-terrorism as a "cyber-enabled activity which intends to advance political, social, or religious ideologies against the public, and cyber dependent activity which further intends to threaten or facilitate damage against the public, properties, and/or systems. Cyber-terrorism has the potential to coincide with traditional terrorism" (Correia, 2022). She introduces a dynamic concept of cyber-terrorism to suit its rapid changes. Also, she requires a particular mens rea, which refers to the radical motivations behind the conduct. The definition clarifies that physical impacts are not the sole requirement of cyber-terrorism; it mentions systems damage that has no physical shape. Thus, she intends, through this definition, to facilitate international legal collaboration to prosecute and counter cyber-terrorism. She, also, points out the impacts of cyber-terrorism on inner society, arguing scholars to study this activity from a collaborative approach to suit the terrorists' illicit use of technology (Correia, 2022).

Conversely, non-violent methods do not reflect cyber-terrorism as it is established that it should result in physical damage regardless of its purposes. As Henschke indicates, the terrorists' mere use of the internet to recruit members or spread their radicalism constitutes a broadcasting activity to deliver their threats to the targeted community (Henschke, 2021). The absence of physical damage deprives these activities of being profiled as cyber-terrorism. Remarkably, Henschke admits that cyberattacks on IoT[11] actuators

[11] The Internet of Things, which means controlling physical equipment by artificial intelligence codes.

impose effects on the victims physically (Henschke, 2021). So, it constitutes cyber-terrorism as it penetrates the connection established by the IoT between the informational internet and physical life. Besides, he argues that the Tallinn Manual prerequisites that the cyberattack impact in the physical world should be perceptible to the present use of force (Schmitt, 2013). The Manual indicates that non-destructive cyber activities are not a use of force, regardless of their moral consequences (Schmitt, 2013).

Dennis Broeders determines that a cyberattack that caused physical damage is not recorded yet (Broeders et al., 2021). He claims that terrorists do not own the required technical and financial skills to accomplish cyberattacks. Besides, the UK legislation requires violence to consider an act as "terrorist"[12] which excludes non-violent acts of this description. In this regard, Stoddart emphasizes that cyber-terrorism threatens national infrastructure in the US since it might include state-supported activities. Also, it might constitute espionage activities which shed light on its gravity though it might not include a violent manner (Stoddart, 2022).

These views reflect a prima facie analysis of cyber-terrorism since they neglect the fact that the moral impacts of this activity exceed their physical counterparts. The national demoralization that cyber-terrorism causes generates hazardous economic and social results that consider it a mala in se activity. Furthermore, cyber-terrorism generates anger among the targeted community that it drives them to demand retaliation by use of force (Shandler et al., 2021) and to respond politically similar to conventional terrorism (Shandler et al., 2021). Also, both sorts of terrorism are motivated by the same psychological incentives.

Ad idem, the Crown Prosecution Service (the UK) stipulates the terror motivation of conduct to consider it "terrorist"[13]. Likewise, the Egyptian Combating Terrorism law decides that the mere mental terrorizing of innocents constitutes a terrorist act, regardless of its physical damage[14]. It decides that the intention of terrorizing civilians to realize the perpetrators' objectives suffices to criminalize their acts under this law. Therefore, national legislations prioritize security concerns by disregarding the condition of physical impacts that Henschke requires (Henschke, 2021). In addition, the Common Position 2001/931/CFSP considers attacks on national infrastructure or governmental facilities terrorist acts, subjecting the perpetrators to counter-terrorism measures[15]. Also, the Austrian Cyber Security Strategy requires the intention to terrorize civilians to inflict damages to national

12 The Terrorism Act 2006, c.11. 2006. https://clck.ru/34Chci

13 Crown Prosecution Service (2021), Terrorism. https://clck.ru/36kt3Z

14 Law No 94/2015, Art 2 para 1.

15 Article 1(3) of Common Position 2001/931/CFSP, see The EU list of persons, groups and entities subject to specific measures to combat terrorism, Factsheet on 14 January 2015. https://clck.ru/36kt4j

infrastructure or economic services to profile an act as a terrorist[16]. Hence, domestic legislations concentrate on the psychological aspect of terrorism since they stipulate the intention to intimidate innocents into this category of criminal acts; it is the distinctive theme of cyber-terrorism that might not cause physical damage and the determinant factor of this category.

Similarly, Margariti argues that the intention to spread terror qualifies an act as a terrorist, regardless of its motives (Margariti, 2017). This element distinguishes terrorism from ordinary crimes. It is a specific mens rea that represents the threshold of this classification. She adopts this standard as a cosmopolitan determinant of the actus reus of international terrorism, which is required to impose a universal legal framework upon it (Margariti, 2017).

So, the non-requirement of the physical impacts to consider an act a terrorist enhances an inclusive theme of cyber-terrorism studies, which aligns with Correia's definition discussed above (Correia, 2022). Although its mere moral consequences, cyber-terrorism threatens world peace and security as it might ignite an armed dispute. Unlike conventional terrorism, individuals can resort to no shelters against cyber-terrorism; the codes that cyber-terrorists employ to jeopardize computing systems within the targeted community penetrate numerous layers of protection. Therefore, this cyber insecurity destabilizes international peace and security. Cyber-terrorism can be elevated to be an enemy to mankind as Perloff-Giles describes (Perloff-Giles, 2018).

2.2. The Contextual Elements of Crimes Against Humanity: Other Inhumane Acts

The Rome Statute includes the term "other inhumane acts" in Article 7(1) (k) to establish the ICC's jurisdiction on these severe acts. This term passed through historical processing by both doctrine and jurisprudence. Yet, the objective of this paper implies focusing on reviewing other inhumane acts elements to construct the comparison required to prove their applicability to cyber-terrorism, as an international illegal activity. Since this term was drafted within international law, it is a must to review its elements from the perspectives of international doctrine and jurisprudence.

Initially, Article 7(1) (k) of the Statute establishes that the classification "other inhumane acts" is a part and parcel of CAH it prohibits (Broeders et al., 2021). This article constructs this act on these pillars: inhumane acts, the intention to cause suffering, mental or physical. They are built on the essential elements of CAH. Still, they show an inclusive approach to prevent disability to prosecute innovative non-included acts.

[16] Federal Chancellery, 'Austria Cyber Security Strategy', 2013, 21. https://clck.ru/36kt6E

Accordingly, Rustam Atadjanov argues that the systematic nature of crimes against humanity distinguishes them from ordinary local criminal behavior (Atadjanov, 2019). So, being an organized behavior reflects the element of context required to profile an act as a crime against humanity. Besides, this systematic nature drives Hobbs argues to argue that CAH express "extraordinary evil" (Hobbs, 2017). Thus, this element represents their severity on humanity's legal interests and their large scale. Nevertheless, Seada Hussein Adem claims that the CAH term suffers a normative gap in the international doctrine that the Statute seeks to bridge by counting the elements that qualify an act as CAH (Adem, 2019). She concludes that the evolution of CAH jurisprudence, as well, bridges this gap since the ad hoc tribunals and the ICC developed an inclusive approach that settled the dilemma (Adem, 2019).

The International Law Commission (ILC) requires the systematic approach of deeds and their widespread to be considered CAH[17]. Besides, it argues that they could be committed by non-state actors[18]. Therefore, the ILC permits classifying the acts committed by groups, or organizations, as CAH, according to the provisions of the Rome Statute. CAH are not perpetrated by states exclusively but by independent bodies or individuals as well. Besides, the ILC requires the multiplicity of victims as a major element of this crime. This condition enhances the widespread requirement and deprives individuals of limited acts of this classification.

Concerning jurisprudence, the term "inhumane acts" reflects the continued evolution of crimes against humanity classification, which was used in 18 cases before the ICC as an alternative response to the legal vacuum (MacNeil, 2021). In Prosecutor v Jean-Pierre Bemba Gombo[19] argues that crimes against humanity have four pillars: a targeted civilian community, scope of the attack, the acts included, mens rea[20]. Besides, the ICC considers inhumane acts that cause mental damages crimes against humanity[21]. In Prosecutor v Germain Katanga and Mathieu Ngudjolo Chui[22] the judges decide that severe violations of fundamental human rights, as established in the international human rights law, are inhumane acts under Art 7(1) (k) of the Statute[23]. John Quigley concludes that this ICC

17 The International Law Commission, Draft Code of Crimes against the Peace and Security of Mankind, 1996 UN Doc. A/51/10 article 18 (k), p 47. https://clck.ru/36kt7d

18 Ibid.

19 Case No. ICC-01/05-01/08.

20 Ibid para 117 and (Park & Switzer, 2020).

21 Ibid, see 'The Elements of Crimes' Published by the International Criminal Court (2013), ISBN 92-9227-232-2, ICC-PIOS-LT-03-002/15_Eng. https://clck.ru/36ktC8

22 ICC-01/04-01/07.

23 Ibid, para 448. The ICC adopts the same principle in Request for authorization of an investigation pursuant to article 15 regarding the situation in the People's Republic of Bangladesh and the Republic of the Union of Myanmar, ICC-01/19, para 128.

Chamber affirms that the contextual elements of other inhumane acts are: intentional great suffering or mental or physical injury (Quigley, 2023). It is an independent category of criminalization that does not require a connection to other included crimes (Quigley, 2023).

Moreover, the International Criminal Tribunal for the former Yugoslavia (ICTY) decides that acts that injure human dignity are "inhumane acts" under the Statute[24]. Thus, the Tribunal extends the interpretation of that term to exceed the Statute, covering novel criminal acts. The Tribunal opinio juris is a result of a doctrine vacuum regarding a disciplined definition of "inhumane acts". Besides, the ICTY stipulates these elements for an act to constitute an inhumane act:

– serious behavior,

– the harm, which may be mental or physical or injury to human dignity,

– and the mens rea[25].

It, also, concludes, in Prosecutor v Milorad Krnojelac[26], that inhumane acts compromise deliberate deeds that inflict severe mental or physical damage to innocents[27]. This jus cogens qualifies perpetrators' acts to be crimes against humanity because of the severity of their impacts. The European Court of Human Rights (ECHR), in Liu v Poland[28] and M.T. and Others v. Sweden[29], utilize the term inhumane to describe acts that degrade a person's dignity and violate his fundamental rights.

Thus, international jurisprudence establishes that these acts are CAH, precisely under the "other inhumane acts" category. It adopts this term as a residual clause to broaden its jurisdiction concerning the prosecution of crimes against humanity to provide effective protection to humanity. Hence, it expresses a flexible jurisprudence to utilize the included legal terminology to contextualize the non-included atrocities under the Rome Statute.

2.3. The applicability of "Other Inhumane Acts" to Cyber-terrorism

The literature on the contextual elements of the term "other inhumane acts" underlines their severity; it comes from their damage to the mental and physical well-being of innocents. The analysis of these elements reflects the unordinary evil of these acts. Thus, other acts that reflect the same evil should be classified as other inhumane acts if the contextual

---

24 Prosecutor v Muci´c et al, Trial judgment, 16 November 1998, IT-96-21-T, (Celebici˘, Trial judgment), paras 521–522.

25 Prosecutor v Karadži´c, Trial judgment, 24 March 2016, IT-95-5/18-T, (Karadži´c, Trial judgment), para 494.

26 IT-97-25-T.

27 Ibid, footnote 382.

28 Application no. 37610/18, on 6 October 2022.

29 Application no. 22105/18, on 20 October 2022.

elements apply. Put differently, the determinant factor of this classification to an act is the applicability of these elements to it.

Initially, cyber-terrorism violates the core principles of IHL (Werle & Jeßberger, 2014). It, first, threatens the minimum standards of humanity by spreading terror. Then, the civilian damages it causes transcend the proportionality standards, predominantly the terrorists' animus nocendi is non-discriminatory. Cyber-terrorists prioritize accomplishing their objectives regardless of innocent civilian sufferings. This nondiscriminatory theme of cyber-terrorism accords with the Rome Statute demonstration of crimes against humanity[30]. The Statute requires that an act should be collected against civilians to constitute a crime against humanity. International jurisprudence admits that the damage of these crimes is both physical and mental. It claims that the mere disregarding of human dignity considerable damage to establishing an accusation[31].

Furthermore, Stella Margariti victimizes the international community regarding cyber-terrorism since it targets international peace and security (Margariti, 2017). Besides, the systematic nature of crimes against humanity that Hobbs points out is shared between cyber-terrorism and crimes against humanity (Hobbs, 2017). Besides, they both have transnational impacts that ground for international involvement. They both constitute a threat to humanity which implies categorizing them in the same classification. Also, as Atadjanov indicates, the element of systematic nature applies to cyber-terrorism since it threatens international peace and security and constitutes a widespread nondiscriminatory organized attack on civilians (Atadjanov, 2019). Indeed, cyber-terrorism generates critical suffering for the international community because the perpetrators intend to jeopardize fundamental human rights. Their systematic manners disrupt the "peaceful cohabitation" (Atadjanov, 2019) of the targeted communities because they negatively affect the concretes of humanity, protected under the UDHR 1948[32]. Furthermore, the systematic nature of CAH, as a contextual element, applies to cyber-terrorism since it threatens international peace and security and constitutes a widespread nondiscriminatory organized attack on civilians.

This opinio juris supports the discussed claim that cyber-terrorism that causes nonphysical damages is a crime against humanity. This conduct targets civilians without discrimination and the perpetrators deliberately ignore civilian casualties to accomplish their objectives. Furthermore, the International Law Commission, in its draft of a convention on the prevention and punishment of crimes against humanity, considers mental harm

30 The Rome Statute, Art 7.

31 Prosecutor v Karadži´c, Trial judgment, 24 March 2016, IT-95-5/18-T, (Karadži´c, Trial judgment), para 494.

32 The Universal Declaration of Human Rights, the United Nations, GA-Res 217/1948. https://clck.ru/36ktDK

adequate to profile an act as a crime against humanity[33]. So, in international law doctrine, physical damage is not a core requirement of crimes against humanity. Similarly, international jurisprudence establishes that mental suffering suffices to qualify perpetrators' acts to be crimes against humanity under Art 7 (1) (k) of the Statute. This approach underlines the gravity of mental damage that cyber-terrorism inflicts.

Nonetheless, Maguir does not require the nondiscriminatory clause to describe an act as a crime against humanity (Maguir, 2022). He argues that they must be systematic against civilian groups with the aware deliberate mens rea of the perpetrators. Likewise, the Appeals Chamber of the UN Special Tribunal of Lebanon pointed out this mens rea should be the intent to spread terror through means that danger civilians[34]. It, also, mentioned that customary international law does not limit terrorism to certain means. Thus, it is admitted that terrorists can utilize cyber tools to achieve their aims. The determinant factor is the public terror intent, regardless of the criminal conduct's shape.

Moreover, Tsilonis addresses that the concept of "organizational policy", that Art 7 (2)(a) of the Rome Statute includes, expands to non-state actors, e.g., terrorists (Tsilonis, 2019). The terror activity might not be state backed but the ICC can prosecute the perpetrators. The purpose of this provision is to enhance humanity's protection against severe crimes. The legal aims of Art 7 implement transcending the literal interpretation of the mentioned term to entail terrorist conduct.

The pillars of inhumane acts coincide with the definition of cyber-terrorism that Correia proposes (Correia, 2022). Both international jurisprudence and doctrine argue that intentional grave acts that target innocent civilians, causing damage to their fundamental rights, regardless of their shape, are inhumane acts under Art 7 of the Rome Statute. Obviously, the examination of these pillars proves their applicability in the context of cyber-terrorism. By targeting national infrastructure, cyber-terrorists affect civilians. Besides, the widespread attack is required to achieve the perpetrators' aims of terrorizing societies, which is the distinctive theme of their activity. Then, the conduct of cyber-terrorists against civilians, regardless of its sort. Finally, the perpetrators should intend to terrorize innocents to achieve their goals. Perloff-Giles's analysis of cyber offenses elements (Perloff-Giles, 2018) accords with the jus cogens that international courts establish, particularly the ECHR illustration of inhumane acts as violations of human rights. Indeed, cyber-terrorism manifests human dignity degrading deeds under this illustration.

---

33 The International Law Commission, "Report of the International Law Commission", Seventy-first session (29 April–7 June and 8 July–9 August 2019) A/74/10, p12. https://clck.ru/36ktFT

34 The UN Special Tribunal of Lebanon Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, 16 February 2011, Case No. STL-11-01/1 (STL Decision).

To conclude, scholars and jurists enhance the doctrine of counting cyber-terrorism as a crime against humanity under the Rome Statute. They target victims systematically and generate serious unlimited impacts. Their transnational consequences provide grounds for international concern. Regardless of its method, the state of terror the perpetrators tend to impose suffices to consider cyber-terrorism a crime against humanity. Also, the extension of the ICC's jurisdiction to prosecute cyber-terrorists profiles their conduct as crimes against humanity. The inhumane acts category entailed in Art 7 (1) (k) of the Rome Statute can include cyber-terrorism. This conclusion implies utilizing universal legal mechanisms under the jurisdiction of the ICC to prosecute cyber-terrorists. Consequently, ruthless cyber-terrorists are subject to the ICC jurisdiction as in the case of other crimes against humanity perpetrators.

3. Universal Jurisdiction in Prosecuting CAH

The evolution of international judicial cooperation innovated the universal principle of jurisdiction. It means the ability to prosecute and try criminals regardless of their location or nationality. It seeks to achieve international justice that requires transcending the traditional jurisdiction determinants to cut-off severe acts of crime. Jovana Blesic constrains the application of universal jurisdiction to international crimes as they impose an erga omnes obligation to prosecute the perpetrators (Blešić, 2022).

Universal jurisdiction presents a significant progression of international criminal justice since it enables states and the concerned bodies to prosecute international criminals globally, regardless of their nationality (Mung'omba, 2022). Thus, universal jurisdiction restricts their impunity which enhances international criminal justice. It constitutes a right of the international community to intervene wherever CAH are committed to prosecuting the perpetrators (Mung'omba, 2022). Notably, Mung'omba mentions that universal jurisdiction does not require a direct link between the prosecuting judicial body and the crime (Mung'omba, 2022). Universal jurisdiction, in his view, "stands out" of the basic jurisdictional norms, which suits its mission in enforcing international criminal justice (Mung'omba, 2022)[35]. It is based on the need to enforce justice and deterrents regarding CAH (Mung'omba, 2022). Thus, universal jurisdiction is crystalized in international law as a unique set of CAH prosecution and trying. On the UN level, states delegations at the 73rd Legal Session decided that universal

[35] See (Mung'omba, 2022). He, however, decides that the perpetrator should be present in persona before the court under the Princeton Principles, ibid 96, see also Global Policy Forum. (2021, June 2). Princeton Principles on Universal Jurisdiction: Princeton Project on Universal Jurisdiction. https://clck.ru/36ktLY

jurisdiction represents an effective toolkit to prosecute core crimes. Among them, they enlisted CAH[36].

Kittichaisaree argues that states impose national jurisdiction on both a subjective and objective basis (Kittichaisaree, 2017). International jurisprudence limits national jurisdiction to traditional factors[37], especially as there is no convention adopting universal jurisdiction. Furthermore, domestic courts should impose their "presumptive jurisdiction" regarding crimes against humanity. Maguir claims that the victims' interests justify the priority of the national prosecution of those crimes (Maguir, 2022). However, Soler criticizes this jurisdiction because it would reflect a power abuse of certain states that deprives a defendant of their right to a fair trial (Soler, 2019). Hence, practicing universal jurisdiction regarding CAH should be equitable and proportionate to guarantee effective justice (Soler, 2019). These conditions maintain the balance between confronting CAH and respecting national sovereignty. Also, he calls for drafting a unified international understanding of aut dedare aut judicare refusal reasons to restrict the impunity of CAH perpetrators, which is considered the major reason for core crimes continuation (Maguir, 2022). This appropriate application of universal jurisdiction, therefore, enhances international criminal justice since it stretches jurisdictional tools to prosecute and extradite CAH perpetrators. Moreover, it supports states to fulfill their obligations concerning prosecuting core crimes, which protects victims' human rights and enhances the traditional understanding of the rule of law (Maguir, 2022). Remarkably, he advocates the right of a third state to prosecute CAH perpetrators as he argues that universal jurisdiction fills up the vacuum caused by the absence of territorial jurisdiction and nationality jurisdiction (Maguir, 2022). Universal jurisdiction, hence, falls under state obligations to prosecute core crimes (Maguir, 2022).

Notwithstanding that universal jurisdiction limits the perpetrators' impunity, it was considered, in certain cases, aggression on national sovereignty and stability[38]. The African Union refused a Spanish arrest warrant against Lieutenant-General Emmanuel Karenzi Karake, considering it a violation of international law and an abuse of the principle of universal jurisdiction. It, also, condemned the European judicial attempts to subordinate the African judiciaries via the

[36] The 6th Committee of the UN General Assembly - Legal (73rd Session), 'The scope and application of the principle of universal jurisdiction (Agenda item 87)', see resolution 72/120. https://clck.ru/36ktQV

[37] See the Lotus Case (France v. Turkey), Judgment of 7 Sept. 1927, Series A No. 10.

[38] African Union Doc PSC.PR/COMM.(DXIX) Communiqué, Peace and Security Council 519th, 26 June 2015, paras 4-5. https://clck.ru/36ktSW

misuse of universal jurisdiction[39]. This statement reflects the controversial theme of universal jurisdiction. Although it is a mechanism to prosecute core crimes, ending their impunity, its application suffers shortages. Nyawo justifies this fact by the absence of an international treaty or instrument that defines universal jurisdiction and explains its applications (Nyawo, 2023). He argues that universal jurisdiction is indispensable to confront CAH since all states have major interests in this (Nyawo, 2023). Furthermore, he justifies universal jurisdiction by the moral global duty that the natural theory includes (Nyawo, 2023, p. 225). This duty obliges the international community to cooperate against the evil deeds that threaten world peace and security. The UNSC mentioned the obligation to prosecute universal crimes and punish the perpetrators universally[40]. This resolution reflects the international interpretation of CAH severity that endorses a universal scheme to prosecute the perpetrators.

Human Rights Watch representative Lotte Leicht argues that the UN developed a mechanism to prosecute CAH perpetrators. It includes a standing prosecutor who initiates the investigations of CAH without establishing an ad hoc court. His jurisdiction extends universally to overcome judicial or political odds[41].

3.1. Aut Dedere Aut Judicare Cyber-terrorism

International jurisprudence affirms that terrorism accusations imply the application of universal jurisdiction due to their severity (Soler, 2019). Since aut dedare aut judicare composes a general principle in international law, the international community should utilize it to confront cyber-terrorism. Its qualitative severity, the deficiency of international human rights protection, and the threat to world peace that cyber-terrorists' impunity support the application of universal jurisdiction by both international and domestic courts to prosecute and extradite them. Then, the international deterrent is guaranteed regarding cyber-terrorism.

According to her profiling of cyber offenders as an enemy to mankind (Perloff-Giles, 2018), Perloff-Giles supports imposing universal jurisdiction to prosecute and extradite cyber-terrorists. Besides, she argues that states can prosecute pirates

39 Ibid para 6.

40 UNSC/S/RES/138, 23 June 1960, para 4. https://clck.ru/36ktdL

41 The European Parliament. (2018, June 28). Workshop: Universal jurisdiction and international crimes: Constraints and best practices. Brussels, EP/EXPO/B/COMMITTEE/FWC/2013-08/Lot8/21.

wherever they are active on the "high seas" under the UNCLOS[42]. Then, she stretches the "high seas" term to include cyberspace as she considers it a transnational sphere of interactions (Perloff-Giles, 2018). She establishes her view on a US court judgment deciding that being on the "high seas" is not a condition to apply universal jurisdiction against piracy[43]. Her comparison shows that both piracy and cybercrime endanger international commerce as cyberattacks can disrupt commercial and financial services websites. So, universal jurisdiction is an effective approach to suppress transnational cybercrimes.

Kittichaisaree claims that technical issues complicate universal jurisdiction support, such as cloud computing as in cyberspace, several states may claim their extraterritorial jurisdiction over cloud-based activities (Kittichaisaree, 2017). As he reviews international legal instruments, he mentions that the permission to extraterritorially prosecute an "unauthorized broadcast" from a vessel located on high seas[44] extends to cyber-facilitated broadcast (Kittichaisaree, 2017). So, he applies the broadcasting term to internet broadcasting websites like Facebook[45] and Twitter[46]. These online platforms are used by terrorists to broadcast their ideologies and recruit their personnel, which provides a reason for states to impose their jurisdictions. Besides, the 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, establish universal jurisdiction regarding criminal acts, which applies to cyber-terrorism, if they target the personnel included in Article 1[47]. It demands the Party States utilize their legal tools to suppress these activities, achieving the Convention's aims. Due to the accelerated development in internet access meanings, cyberterrorism is cheap if compared to its impacts (Kittichaisaree, 2017). Thus, the Budapest Convention on Cybercrime should be universalized to establish a global network, facilitating the prosecution of cyber-terrorists.

As Maguir argues, prosecuting cyber-terrorism by a national court proves efficient as it is motivated by the victims' trust in their courts[48]. Besides, the presumptive jurisdiction reflects, at its core, imposing universal jurisdiction over these crimes; it

---

42 Article 101 c of the United Nations Convention on the Law of the Sea, 1833 U.N.T.S. 397 (entered into force Nov. 16, 1994).

43 United States v. Ali, 718 F.3d 929, 935-38 (D.C. Cir. 2013).

44 Art 109, the UNCLOS.

45 The organization is recognized as extremist, its activity is prohibited in the territory of the Russian Federation.

46 A social network blocked in the territory of the Russian Federation for disseminating illegal information.

47 Art 3 of the 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, entered into force on 20 February 1977.

48 See the Lotus Case (France v. Turkey), Judgment of 7 Sept. 1927, Series A No. 10.

prevents the victims from jurisdictional vulnerabilities related to cyber-terrorism prosecution (Kittichaisaree, 2017). Hence, this attitude complies with the extraterritorial punishment of cyber perpetrators, regardless of their location or nationality. Nonetheless, the transnational impacts of cyber-terrorism may involve several jurisdictions that lead to their conflict. So, the complementarity principle of the ICC retains its significance to cure state authorities' deficiency in cyber-terrorism prosecution. Yet, this system of fallback complementarity expresses the vertical order between the ICC and its Members to prosecute core crimes (Burens, 2016). So, Laura Burens argues that a horizontal inter-state mechanism of complementarity enhances universal jurisdiction to prosecute these crimes under the Statute. Besides, she introduces the state where the perpetrator is located as the obliged member to utilize universal jurisdiction in the prosecution process (Burens, 2016). This integration of vertical and horizontal complementarity eliminates the odds before universal jurisdiction due to the transparency of the subsidiarity principle (Burens, 2016, p. 89)[49]. Also, Resolution 72/120 mentions that the utilization of universal jurisdiction should fall under international law and the subsidiarity principle to prevent its abuse or inefficiency[50]. Soler, for his part, claims that this integration is required for the adequate application of universal jurisdiction to overcome the deficiency of the subsidiarity principle (Soler, 2019).

Regarding national laws, the UK Legislation extends its jurisdiction over terrorism crimes, regardless of their actus reus, according to the purposes entitled in article 63B[51]. This extraterritorial jurisdiction enhances protection against cyber-terrorism; the Crown Prosecution Service can utilize its legal tools to prosecute the perpetrators extraterritorially[52] if their mens rea was included in the mentioned article. Furthermore, the UK judiciary in R v. Kumar Lama[53], outlined that a domestic court should utilize universal jurisdiction to prosecute grave crimes. Though, Hovell criticizes this trial because of shortages of abroad evidence gathering that led the court to consider Colonel Lama not guilty[54]. Likewise, Combating Information Technology

49 L. Burens claims that this principle maintains the balance between states sovereignty and the international interest to prosecute core crimes.

50 Resolution 72/120, Supra 17.

51 Terrorism Act 2000, the UK, 63A- 63D.

52 The Crown Prosecution Service (2021), 'Jurisdiction', (CPS: Legal Guidance on 26 July 2021). https://clck.ru/36ktjD

53 Case no. 2013/05698 (Central Criminal Court, London, 2016).

54 Hovell, D. (2017, April 6). The 'Mistrial' of Kumar Lama: Problematizing Universal Jurisdiction. EJIL Talk – Blog of the European Journal of International Law. https://clck.ru/36ktkR

Crimes Law[55] extended the Egyptian jurisdiction largely over cybercrimes to include offenses committed by non-nationals provided that[56]:

– the crime was committed on board any naval or aerial or land transportation registered in Egypt or raising its flag;

– the victim is Egyptian;

– the crime was planned or surveilled or funded in Egypt;

– the criminal is an organized group working in several countries among them Egypt;

– the crime might harm any of Egypt's interests or security or any citizen's or residents' interests or security;

– the criminal was found in Egypt after committing the crime and was not yet extradited.

This broad approach by the Egyptian Legislator is a result of the legal vacuum that the Egyptian judges suffered regarding cyber-terrorism. Indeed, it manifests a comprehensive view of the application of universal jurisdiction in cyberspace to enhance the legal protection against cyber-terrorism.

To conclude, the transnational nature of cyber-terrorism, along with its severity on international peace and security, pushes the international community to adopt universal jurisdiction to prosecute and punish the perpetrators. It is a suitable mechanism to confront them because it aligns with the obligations of the state to prosecute core crimes, as recognized in international customary law. Indeed, the ongoing impunity of cyber-terrorists leads to an increase in their crimes. So, the international community should unify its legal efforts to develop a unified global understanding of universal jurisdiction to avoid the legal vacuum.

4. Bridging the Gap

It is recognized that cyber-terrorism is a major sort of illegal activity in cyberspace due to the capabilities provided by the latter; its ambiguous nature, which extends through the real world, allows them to roam and work effectively for their objectives. This manner crystallizes the international theme of cyber-terrorism which requires the utilization of international legal mechanisms to confront. However, the international character of these tools might introduce them as intervention schemes in the internal affairs of independent states. Put simply, states might oppose them justifying that on a sovereignty basis. This fact creates a dilemma concerning prosecuting and trying cyber-terrorists and, also, enhances their impunity in the actual international legal practice. Thus, world peace and security become more fragile against their threats. So, these international mechanisms require

[55] Law No 175/2018.

[56] Ibid pt 1 Art 3.

a firm legal basis to overcome states' opposition and persuade them to cooperate against cyber-terrorism as an international danger.

4.1. Explaining the Dilemma

The application of international legal norms, regardless of their stability, is yet to be palatable. Interests of states and their interpretation of international law concepts complicate creating a unified manner of the application of international jus cogens. Regarding the research question, international legal practice discloses that both international law norms, the R2P and universal jurisdiction, are continuously refuted. Skeptics are either jurists or diplomatic statements. They reflect the absence of a unified international understanding of these theories. Thus, trying to establish universal jurisdiction on the R2P theory is unfruitful unless the research contains its critiques and contextualizes them within its trajectory.

International legal practice reveals that the application of universal jurisdiction to confront cyber-terrorism is yet to be palatable. States, and even international organizations, might oppose it and frustrate foreign legal measures adopting universal jurisdiction as a basis. This opposition appears apparently in the statement of the African Union when the organization claimed that universal jurisdiction violated the stability of the whole continent[57]. Although the judicial measures were taken by a European court to prosecute CAH in Rwanda, they were reviewed in a merely political context relevant to the European colonization of Africa memories. Such attitudes enhance the perpetrators' impunity and hinder the enforcement of justice.

Furthermore, at the 12th Meeting of the Sixth Committee of the UN General Assembly, the representatives' discussions reveal a considerable gap regarding universal jurisdiction. While Germany presented the judicial experience of a domestic court in prosecuting CAH committed by Syrian officials[58], Columbia stipulated that the application of universal jurisdiction should be under a bilateral or international treaty[59]. The majority of the representatives pointed out that the effectiveness of universal jurisdiction requires its incorporation within national legal systems[60]. This report crystalizes the diversion of states' attitudes towards universal jurisdiction that deepens the gap in its conceptualization and application. Besides, states might oppose universal jurisdiction since they might neither permit a foreign jurisdiction to prosecute a cyber-terrorist within their territory nor extradite a national terrorist to a foreign

57 African Union Doc PSC.PR/COMM.(DXIX) Communiqué, Peace and Security Council 519th, 26 June 2015, paras 4-5. https://clck.ru/36ktSW

58 Speakers Disagree on How, When, Where Universal Jurisdiction Should Be Engaged, as Sixth Committee Takes up Report on Principle. (2022, October 12). UN Press. https://clck.ru/36ktp8

59 Ibid para 7.

60 Ibid paras 3, 4, 5 & 8.

jurisdiction. In addition, Blešić claims that political will is the determinant factor of universal jurisdiction application (Blešić, 2022). It depends on the existence of bilateral treaties between states.

Moreover, the decentralization of international criminal justice enforcement leaves universal jurisdiction relying merely on states' will and actions (Nyawo, 2023). This presents a crucial deficiency in it as it might lead to political conflicts between states, particularly under the absence of international guiding rules about universal jurisdiction. Thus, drafting an international legal instrument is a must to stabilize the judicial status regarding CAH prosecution. So, to overcome this barrier, universal jurisdiction requires a universal justification that accords with its purposes and nature.

International doctrine points out that the R2P theory has several critiques. Royer notes that international law practice reveals that states might profile the R2P principle as a reflection of Western imperialism (Royer, 2021). He argues that the utilization of the R2P theory to justify military interventions against CAH promoted this picturization of that humanitarian theory (Royer, 2021). Also, the R2P would threaten the balance between justice and order (Royer, 2021), which leads to chaos within the targeted state. This dichotomy is the basis of the R2P critiques (Royer, 2021). Therefore, he suggests that jurists should focus on that aspect of the R2P to guarantee the impartiality of its utilization (Royer, 2021). Furthermore, he argues that doctrine should judge the intervention under the R2P according to each case separately (Royer, 2021) as the selective application might trigger injustice in international legal practice (Royer, 2021). The generalization of judging the R2P endangers the reliability of this humanitarian concept; its misuse should never permit its abandonment. So, to overcome this obstacle, the circumstances of each case per se are the determinant of the R2P utilization. This mechanism liberates this principle from the states' political will and enhances its impartial application. Lastly, Royer considers the critiques of the R2P a failure to estimate the consequences of evil that this theory confronts.

Hence, the need to adopt universal jurisdiction against cyber-terrorism exceeds the states' limited opposition. This international criminal act requires the utilization of international toolkits that transcend domestic legal borders and prosecute cyber-terrorists regardless of their location. The R2P theory is the appropriate justification to impose universal jurisdiction regarding cyber-terrorism.

4.2. The Solution: The Validity of the R2P to Impose Universal Jurisdiction Against Cyber-Terrorism

Doctrine considers cyber-terrorism an international evil because of its impacts (Margariti, 2017). Its severity on world peace and security matches the ordinary CAH. The international community is the victim of both crimes (Margariti, 2017). However, its cyber theme distinguishes it as a modern enemy to humanity (Perloff-Giles, 2018). It is an evolved sort

of CAH that falls under the category: other inhumane acts. The congruence of cyber-terrorism elements with the contextual elements of CAH, as jurisprudence concludes[61], solids this categorization. Hence, it requires universal jurisdiction as a global mechanism to prosecute and extradite terrorists. Still, due to the opposition to universal jurisdiction[62], it requires a firm pillar to justify its application that overcomes these obstacles. This pillar is the R2P theory.

The previous review of doctrine points out the prominence of the R2P theory in international law. It was developed into a tool to defend humanity. The R2P's fundamental purpose is protecting humanity against atrocities. Thus, its employment to confront CAH proves its worth in international doctrine and jurisprudence. The R2P, as Royer introduces, is a humanitarian tool to prevent evil since it justifies legal intervention to haunt CAH perpetrators (Royer, 2021). It prioritizes protecting individual human beings rather than maintaining sovereignty under the Westphalian understanding[63].

Royer praises the flexible theme of the R2P as it harmonizes its application with the humanitarian needs to prevent CAH (Royer, 2021). He presents a moral reframing of the R2P as he constructs it based on confronting evil (Royer, 2021). As a consequence, political will cannot oppose norms that are built on it. Instead, the R2P combines states' political interests and humanity's morals in a shield against evil (Royer, 2021). De facto, it is a political moral R2P that defends individuals against evil deeds (Royer, 2021). This reframing of the R2P proves its validity to utilize other international law norms to suppress CAH. Remarkably, Royer's vision of the R2P harmonizes it with state sovereignty; the latter, at its core, is a shield against evil as it organizes the autonomous administration of internal affairs. Hence, it limits national disorder that evil could exploit to spread (Royer, 2021). So, sovereignty reflects the state's responsibility to protect individuals against evil.

As the ICC practice discloses, the collective obligation on states exhorts them to adopt universal toolkits to eradicate CAH to secure world peace[64]. The nature of universal jurisdiction is compatible with this purpose; prosecuting CAH internationally limits their occurrence and enhances justice. Since the R2P justifies military intervention against CAH, it rather justifies judicial intervention, i.e., imposing universal jurisdiction. As the research concludes that cyber-terrorism is a CAH, the R2P should justify prosecuting cyber-terrorists universally. This conclusion implies that a court or a sole prosecutor can prosecute a

---

61 Prosecutor v Muci´c et al, Trial judgment, 16 November 1998, IT-96-21-T, (Celebici˘, Trial judgment), paras 521–522; Prosecutor v Karadži´c, Trial judgment, 24 March 2016, IT-95-5/18-T, (Karadži´c, Trial judgment), para 494; IT-97-25-T.

62 Discussed in the previous section.

63 Resolutions 1674 (2006), 63/308 (2009)68 and 1894 (2009).

64 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (BiH v Serbia and Montenegro), 26 February 2007, ICJ Reports 2007 p. 43, para 166.

cyber-terrorist located within another jurisdiction if the territorial jurisdiction is lax in that. The horizontal complementarity applies in this case according to Burens's explanation (Burens, 2016). The R2P justifies this judicial intervention because of the international community's duty to prevent CAH as established in international customary law. Judicial intervention to confront CAH is better than military intervention since it enhances global trustworthiness in international criminal justice and eliminates cyber-terrorists' threats to humanity.

Conclusion

The research studies the R2P norm and analyzes its pillars to create a comprehensive image of it in international law. It is a preventive instrument that protects humanity against atrocities. Its firmness could be concluded from its continuous adoption by the UNSC and the international community to intervene to suppress CAH. It is a general principle in international law. Furthermore, legal analysis proves the flexible feature of the R2P since its employment should be on a case-by-case basis. Being utilized to justify military operations permits the R2P to justify legal intervention to prosecute CAH. These facts prove the suitability of the R2P for this mission.

Also, the research analyzes cyber-terrorism. It is a modern criminal activity that inflicts damage on states. Doctrine considers it a mutual enemy to humanity as it threatens world peace and security. By analyzing its elements, the research compares them to the contextual elements of CAH. It concludes the congruence between them. This means that cyber-terrorism is a CAH under the Rome Statute. The category of other inhumane acts extends to include cyber-terrorism. Hence, the international community should act to prosecute and punish cyber-terrorists to eradicate their impunity.

External judicial intervention is achieved in international private law through universal jurisdiction. It includes utilizing domestic judicial tools within other jurisdictions. So, it faces several obstacles from states and even regional organizations. These obstacles frustrate international legal efforts to suppress cyber-terrorism. This fact implies finding a suitable legal justification for universal jurisdiction. A justification that paves the way for the international community to prosecute cyber-terrorists.

Then, the research introduces the R2P principle as the required justification for universal jurisdiction regarding cyber-terrorism. Since the latter is an international threat to world peace and security, the international community must act to eradicate its dangers via universal jurisdiction mechanisms. This intervention complies with international law because it safeguards human rights, which is its favored interest.

Finally, the research closes the gap between international public law and international private law; it employs the R2P theory from the former to justify universal jurisdiction from

the latter. This combination manifests the complementarity of international law branches, which is required to produce a strong understanding of international cyber issues.

References

Adem, S. H. (2019). Palestine and the International Criminal Court. In Werle, G., & Vormbaum, M. (Eds.), *International Criminal Justice Series*, *21*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-291-0

Albahar, M. (2019). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Science and Engineering Ethics*, *25*(4). https://doi.org/10.1007/s11948-016-9864-0

Atadjanov, R. (2019). Humanness as a Protected Legal Interest of Crimes Against Humanity. Conceptual and Normative Aspect. In G. Werle, & M. Vormbaum (Eds.), *International Criminal Justice Series*, *22*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-299-6

Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. *Social Science and Public Policy*, *54*, 138. https://doi.org/10.1007/s12115-017-0114-0

Azubuike, E. C. (2023). Principle of Responsibility to Protect: Implications for Sovereignty. In E. Duruigb, R. Chibueze, & S. G. Ogbodo (Eds.), *International Law and Development in the Global South* (pp. 55–77). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-13741-9_5

Bellamy, A. (2018). Responsibility to Protect: Justice and Responsibility—Related but Not Synonymous. In J. Waterlow & J. Schuhmacher (Eds.), *War Crimes Trials and Investigations* (pp. 263–299). Cham, Switzerland: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-64072-3_9

Blešić, J. (2022). Aut Dedere Aut Judicare in International and Domestic Law. In *Protection of human rights and freedoms in light of international and national standards, Contemporary Problems of the Legal System of Serbia* (pp. 213–224). The Faculty of Law, University of Belgrade.

Broeders, D., Cristiano, F., & Weggemans, D. (2021). Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy, *Studies in Conflict and Terrorism*. https://doi.org/10.1080/1057610x.2021.1928887

Burens, L. (2016). Universal Jurisdiction Meets Complementarity: An Approach towards a Desirable Future Codification of Horizontal Complementarity between the Member States of the International Criminal Court. *Criminal Law Forum*, *27*(1), 75–97. https://doi.org/10.1007/s10609-016-9272-9

Cantini, N., & Zavialov, D. (2018). Fixing Responsibility to Protect: Lessons from and Proposals for the Case of Libya. *Peace Human Rights Governance*, *2*(1), 75. https://doi.org/10.14658/pupj-phrg-2018-1-4

Correia, V. J. (2022). An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom, *SN Computer Sciences*, *3*, 84. https://doi.org/10.1007/s42979-021-00962-5

Delerue, F., Desforges, A., & Géry, A. (2019, April 23). A Close Look at France's New Military Cyber Strategy. *War on the Rocks*. https://clck.ru/36ktrj

Ercan, P. G. (2022). *The Responsibility to Protect Twenty Years On: Rhetoric and Implementation*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-90731-0

Fehl, C. (2015). Probing the Responsibility to Protect's Civilian Dimension: What Can Non-Military Sanctions Achieve? In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 39–57). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1.

Henschke, A. (2021). Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat. In A. Henschke, A. Reed, S. Robbins, & S. Miller (Eds.), *Counter-Terrorism, Ethics and Technology' Advanced Sciences and Technologies for Security Applications*. Springer. https://clck.ru/36ktsa

Hobbs, H. (2017). Towards a Principled Justification for the Mixed Composition of Hybrid International Criminal Tribunals. *Leiden Journal of International Law*, *30*(1), 177. https://doi.org/10.1017/s092215651600056x

Holvoet, M., & Mema, M. (2015). The International Criminal Court and the Responsibility to Protect. In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 21–38). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1. https://doi.org/10.1057/9781137364401_3

Kittichaisaree, K. (2017). Future Prospects of Public International Law of Cyberspace. In K. Kittichaisaree, *Public International Law of Cyberspace* (pp. 335–356). Springer. https://clck.ru/36ktuq

MacNeil, G. (2021). Legality Matters: Crimes Against Humanity and the Problems and Promise of the Prohibition on Other Inhumane Acts. In G. W., & M. Vormbaum (Eds.), *International Criminal Justice Series*, 28. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-443-3

Maguir, R. (2022). Prosecuting Crimes Against Humanity: Complementarity, Victims' Rights and Domestic Courts. *Criminal Law and Philosophy*, *17*, 669–689. https://doi.org/10.1007/s11572-022-09648-2

Margariti, S. (2017). Defining International Terrorism: Between State Sovereignty and Cosmopolitanism. In G. Werle, L. Fernandez, & M. Vormbaum (Eds.), *International Criminal Justice Series*, *15* (pp. 1–26). T.M.C. Asser Press, The Hague. ISBN 978-94-6265-204-0. https://clck.ru/36ktwV

Mung'omba, I. (2022). Universal Jurisdiction as a Tool in Promoting Accountability for International Crimes in Africa: Exploring the Significance of Hissene Habre's Conviction. In E. C. Lubaale, & N. Dyani-Mhango (Eds.), *National Accountability for International Crimes in Africa* (pp. 91–114). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-88044-6_4

Nyawo, J. (2023). The Scope and Application of Universal Jurisdiction: A Synopsis of African States' Positions and Proposals During Plenary Sessions in the Sixth Committee of the United Nations General Assembly. In T. B. K. Sendze, A. Adeboyejo, S. Ugwu, & H. Morrison (Eds.), *Contemporary International Criminal Law Issues. Contributions in Pursuit of Accountability for Africa and the World* (pp. 213–262). Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-555-3_7

Park, T. J., & Switzer, M. (2020, May). R2P & Cyberspace: Sovereignty as a Responsibility. In *The 12th International Conference on Cyber Conflict*. Tallin, Estonia. https://doi.org/10.23919/cycon49761.2020.9131729

Perloff-Giles, A. (2018). Transnational Cyber Offenses: Overcoming Jurisdictional Challenges. *Yale Journal of International Law*, *43*(4), 191–227. https://clck.ru/36ktyQ

Quigley, J. (2023). Prohibition of Palestine Arab Return to Israel as a Crime Against Humanity. *Criminal Law Forum*, *38*. https://doi.org/10.1007/s10609-022-09450-8

Royer, Ch. (2021). A Responsibility to Protect Humanity from Evil. In *Evil as a Crime Against Humanity. Ser. International Political Theory* (pp. 81–130). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-53817-0_3

Schmitt, M. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2021). Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment, *British Journal of Political Science*. https://doi.org/10.1017/s0007123420000812

Soler, Ch. (2019). *The Global Prosecution of Core Crimes under International Law*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-335-1

Stoddart, K. (2022). Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. In K. Stoddart (Ed.), *Cyberwarfare: Threats to Critical Infrastructure* (pp. 351–399). Springer International Publishing. https://doi.org/10.1007/978-3-030-97299-8_6

Tsilonis, V. (2019). *The Jurisdiction of the International Criminal Court.* Springer Nature Switzerland, Gewerbestrasse, Switzerland. https://doi.org/10.1007/978-3-030-21526-2

Werle, G., & Jeßberger, F. (2014). *Principles of International Criminal Law* (4th ed.). Oxford University Press. ISBN 9780198826859. https://goo.su/Xwzm

Wyatt, S. J. (2019). The Responsibility to Protect and Habermas: Theory of Constitutionalisation with a "Cosmopolitan Purpose". In *The Responsibility to Protect and a Cosmopolitan Approach to Human Protection* (pp. 151–176). New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-00701-0_6

Author information

Yassin Abdalla Abdelkarim – Judge, Luxor Elementary Court
Address: New Casalovy Hotel Street, Akhmim Sohag Street, Madinat Nasser, 82516, Sohag, Egypt
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Conflicts of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt –July 23, 2023
Date of approval – October 25, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:343.3/.7:341.4:343.9
EDN: https://elibrary.ru/cmvqzx
DOI: https://doi.org/10.21202/jdtl.2023.43

Применение концепции «обязанность защищать» (R2P) для введения универсальной юрисдикции в отношении кибертерроризма

Яссин Абдалла Абделькарим

Суд общей юрисдикции в Луксоре
г. Сохаг, Египет

Ключевые слова

кибербезопасность,
киберпространство,
кибертерроризм,
международное публичное право,
международное частное право,
права человека,
право,
преступления против человечности,
цифровые технологии,
юрисдикция

Аннотация

Цель: развитие беспроводных технологий и цифровой инфраструктуры радикальным образом изменило среду обитания человечества, порождая новый тип пространства – киберпространство. Уникальность и особенности этой среды, включая анонимность, безграничность, проблемы, связанные с определением и установлением юрисдикции, стали питательной средой для появления новой глобальной угрозы – кибертерроризма, характеризующегося высоким уровнем латентности, низким уровнем раскрываемости и несравнимо большей опасностью, нежели преступления «в реальном мире». Противодействие новым формам преступности потребовало разработки универсальных инструментов, преодолевающих ограничения традиционной юрисдикции и позволяющих государствам преследовать террористов в киберпространстве. Определение соответствующих инструментов и выявление препятствий политико-юридического характера по их реализации является целью проведенного исследования.

Методы: для достижения поставленной цели используется, прежде всего, формально-юридический метод, применяемый для анализа правовых источников, к которым относятся судебная практика, национальное законодательство и международные акты. Также был задействован доктринальный подход, позволивший на основе научных трудов и теоретических конструкций объяснить сложность новых явлений современного мира и спрогнозировать их развитие в будущем. Основное внимание при этом уделяется стороне преступника, чтобы доказать ее антагонизм с человечеством в соответствии с теоретическими взглядами. Наконец, в исследовании анализируются теории универсальной и традиционной юрисдикции, а также то, как они применяются для преследования террористов.

Результаты: в работе дается критический анализ переосмысления и адаптации концепции юрисдикции применительно к глобальной, безграничной и децентрализованной цифровой среде (киберпространство) и противодействию новым формам терроризма (кибертерроризм); приводятся различные юрисдикционные модели, применимые в киберпространстве; преодолевается разрыв между основными отраслями права: международным частным и публичным правом – путем установления взаимосвязи в отношении к кибертерроризму двух теорий: концепций «обязанности защищать» (R2P) и применения универсальной юрисдикции; выявлены тенденции развития универсальной юрисдикции.

Научная новизна: исследование развивает накопленные научные знания в части обоснования введения иностранной юрисдикции на территории государства для преследования кибертеррористов; устанавливается связь между теориями универсальной юрисдикции в международном частном праве и «обязанностью защищать» (R2P) в международном публичном праве; при этом последняя признается в качестве пригодной основы для введения универсальной юрисдикции в отношении кибертерроризма; переосмысливаются такие традиционные понятия, как суверенитет и юрисдикционная независимость. Устраняется пробел в знаниях, связанных с рассмотрением кибертерроризма как преступления против человечности в международном праве.

Практическая значимость: реализация предложенных выводов будет способствовать усилению международного преследования кибертерроризма; гармонизации международного и внутригосударственного правового инструментария в отношении данного преступления.

Для цитирования

Абделькарим, Я. А. (2023). Применение концепции «обязанность защищать» (R2P) для введения универсальной юрисдикции в отношении кибертерроризма. *Journal of Digital Technologies and Law*, *1*(4), 994–1022. https://doi.org/10.21202/jdtl.2023.43

Список литературы

Adem, S. H. (2019). Palestine and the International Criminal Court. In Werle, G., & Vormbaum, M. (Eds.), *International Criminal Justice Series*, *21*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-291-0

Albahar, M. (2019). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Science and Engineering Ethics*, *25*(4). https://doi.org/10.1007/s11948-016-9864-0

Atadjanov, R. (2019). Humanness as a Protected Legal Interest of Crimes Against Humanity. Conceptual and Normative Aspect. In G. Werle, & M. Vormbaum (Eds.), *International Criminal Justice Series*, *22*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-299-6

Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. *Social Science and Public Policy*, *54*, 138. https://doi.org/10.1007/s12115-017-0114-0

Azubuike, E. C. (2023). Principle of Responsibility to Protect: Implications for Sovereignty. In E. Duruigb, R. Chibueze, & S. G. Ogbodo (Eds.), *International Law and Development in the Global South* (pp. 55–77). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-13741-9_5

Bellamy, A. (2018). Responsibility to Protect: Justice and Responsibility—Related but Not Synonymous. In J. Waterlow & J. Schuhmacher (Eds.), *War Crimes Trials and Investigations* (pp. 263–299). Cham, Switzerland: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-64072-3_9

Blešić, J. (2022). Aut Dedere Aut Judicare in International and Domestic Law. In *Protection of human rights and freedoms in light of international and national standards, Contemporary Problems of the Legal System of Serbia* (pp. 213–224). The Faculty of Law, University of Belgrade.

Broeders, D., Cristiano, F., & Weggemans, D. (2021). Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy, *Studies in Conflict and Terrorism*. https://doi.org/10.1080/1057610x.2021.1928887

Burens, L. (2016). Universal Jurisdiction Meets Complementarity: An Approach towards a Desirable Future Codification of Horizontal Complementarity between the Member States of the International Criminal Court. *Criminal Law Forum*, *27*(1), 75–97. https://doi.org/10.1007/s10609-016-9272-9

Cantini, N., & Zavialov, D. (2018). Fixing Responsibility to Protect: Lessons from and Proposals for the Case of Libya. *Peace Human Rights Governance*, *2*(1), 75. https://doi.org/10.14658/pupj-phrg-2018-1-4

Correia, V. J. (2022). An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom, *SN Computer Sciences*, *3*, 84. https://doi.org/10.1007/s42979-021-00962-5

Delerue, F., Desforges, A., & Géry, A. (2019, April 23). A Close Look at France's New Military Cyber Strategy. *War on the Rocks*. https://clck.ru/36ktrj

Ercan, P. G. (2022). *The Responsibility to Protect Twenty Years On: Rhetoric and Implementation*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-90731-0

Fehl, C. (2015). Probing the Responsibility to Protect's Civilian Dimension: What Can Non-Military Sanctions Achieve? In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 39–57). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1.

Henschke, A. (2021). Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat. In A. Henschke, A. Reed, S. Robbins, & S. Miller (Eds.), *Counter-Terrorism, Ethics and Technology' Advanced Sciences and Technologies for Security Applications*. Springer. https://clck.ru/36ktsa

Hobbs, H. (2017). Towards a Principled Justification for the Mixed Composition of Hybrid International Criminal Tribunals. *Leiden Journal of International Law*, *30*(1), 177. https://doi.org/10.1017/s092215651600056x

Holvoet, M., & Mema, M. (2015). The International Criminal Court and the Responsibility to Protect. In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 21–38). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1. https://doi.org/10.1057/9781137364401_3

Kittichaisaree, K. (2017). Future Prospects of Public International Law of Cyberspace. In K. Kittichaisaree, *Public International Law of Cyberspace* (pp. 335–356). Springer. https://clck.ru/36ktuq

MacNeil, G. (2021). Legality Matters: Crimes Against Humanity and the Problems and Promise of the Prohibition on Other Inhumane Acts. In G. W., & M. Vormbaum (Eds.), *International Criminal Justice Series*, 28. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-443-3

Maguir, R. (2022). Prosecuting Crimes Against Humanity: Complementarity, Victims' Rights and Domestic Courts. *Criminal Law and Philosophy*, *17*, 669–689. https://doi.org/10.1007/s11572-022-09648-2

Margariti, S. (2017). Defining International Terrorism: Between State Sovereignty and Cosmopolitanism. In G. Werle, L. Fernandez, & M. Vormbaum (Eds.), *International Criminal Justice Series*, *15* (pp. 1–26). T.M.C. Asser Press, The Hague. ISBN 978-94-6265-204-0. https://clck.ru/36ktwV

Mung'omba, I. (2022). Universal Jurisdiction as a Tool in Promoting Accountability for International Crimes in Africa: Exploring the Significance of Hissene Habre's Conviction. In E. C. Lubaale, & N. Dyani-Mhango (Eds.), *National Accountability for International Crimes in Africa* (pp. 91–114). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-88044-6_4

Nyawo, J. (2023). The Scope and Application of Universal Jurisdiction: A Synopsis of African States' Positions and Proposals During Plenary Sessions in the Sixth Committee of the United Nations General Assembly. In T. B. K. Sendze, A. Adeboyejo, S. Ugwu, & H. Morrison (Eds.), *Contemporary International Criminal Law Issues. Contributions in Pursuit of Accountability for Africa and the World* (pp. 213–262). Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-555-3_7

Park, T. J., & Switzer, M. (2020, May). R2P & Cyberspace: Sovereignty as a Responsibility. In *The 12th International Conference on Cyber Conflict*. Tallin, Estonia. https://doi.org/10.23919/cycon49761.2020.9131729

Perloff-Giles, A. (2018). Transnational Cyber Offenses: Overcoming Jurisdictional Challenges. *Yale Journal of International Law*, *43*(4), 191–227. https://clck.ru/36ktyQ

Quigley, J. (2023). Prohibition of Palestine Arab Return to Israel as a Crime Against Humanity. *Criminal Law Forum*, *38*. https://doi.org/10.1007/s10609-022-09450-8

Royer, Ch. (2021). A Responsibility to Protect Humanity from Evil. In *Evil as a Crime Against Humanity. Ser. International Political Theory* (pp. 81–130). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-53817-0_3

Schmitt, M. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2021). Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment, *British Journal of Political Science*. https://doi.org/10.1017/s0007123420000812

Soler, Ch. (2019). *The Global Prosecution of Core Crimes under International Law*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-335-1

Stoddart, K. (2022). Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. In K. Stoddart (Ed.), *Cyberwarfare: Threats to Critical Infrastructure* (pp. 351–399). Springer International Publishing. https://doi.org/10.1007/978-3-030-97299-8_6

Tsilonis, V. (2019). *The Jurisdiction of the International Criminal Court*. Springer Nature Switzerland, Gewerbestrasse, Switzerland. https://doi.org/10.1007/978-3-030-21526-2

Werle, G., & Jeßberger, F. (2014). *Principles of International Criminal Law* (4th ed.). Oxford University Press. ISBN 9780198826859. https://goo.su/Xwzm

Wyatt, S. J. (2019). The Responsibility to Protect and Habermas: Theory of Constitutionalisation with a "Cosmopolitan Purpose". In *The Responsibility to Protect and a Cosmopolitan Approach to Human Protection* (pp. 151–176). New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-00701-0_6

Сведения об авторе

Абделькарим Яссин Абдалла – судья, суд общей юрисдикции в Луксоре
Адрес: 82516, Египет, г. Сохаг, Мадинат Нассер, ул. Ахмим Сохаг, Нью Касалови Хотел
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.77.51 / Отдельные виды преступлений
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 23 июля 2023 г.
Дата одобрения после рецензирования – 25 октября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.44

Legal Nature of Smart Contracts: Contract or Program Code?

Gergana Varbanova

University of National and World Economy;
Arbitration Court of the BIA
Varna, Bulgaria

Keywords

blockchain,
civil law,
commercial law,
contract law,
contract,
digital technologies,
information technologies,
law,
program code,
smart contract

Abstract

Objective: due to the rapid technological changes, digital economy and contractual relations determine law transformation and legislation development towards adaptation to prospective spreading and application of smart contracts in civil and commercial turnover. In this regard, the study focuses on determining the legal essence of smart contracts as a fundamental step towards the development of their timely and clear regulation.

Methods: the research is based on the methodology of formal-legal and comparative legal analysis. It compares the current Bulgarian legislation with supranational legal sources and identifies the characteristic features of smart contracts as demanded instruments necessary for modern law and economy. The article also compares them with the classical understanding of contracts, making it possible to understand and define the nature of smart contracts more accurately.

Results: it was determined that a smart contract is a software code in which the parties predetermine conditions under which the contractual relationship between them is created, modified and terminated. The research proved that the contract execution does not depend on the action or inaction of its parties, but rather on the occurrence of a predetermined condition (a certain fact relevant to the parties) under which the contract must self-execute. It was substantiated that the will of the parties cannot be changed or replaced because of the special way in which the smart contract is recorded in a distributed ledger. It is found that the fundamental problem of transferring the will from the legal language to the program code of the smart contract persists: if the will of the parties is incorrectly transferred to the program code, the smart contract may self-execute, but its execution will not be the result that the parties counted on.

Scientific novelty: the analysis made it possible to compare the current national (Bulgarian) legislation and supranational (European) law. It revealed the vagueness of smart contracts regulation, both at the national and international level, and identified a number of issues in need of scientific and legal interpretation, which refer to the legal nature of smart contracts in view of the self-executing program code concept.

Practical significance: the study can serve as a basis for further development of legislation towards its adaptation to the prospects of smart contracts spreading and application in civil and commercial turnover. It also allows an in-depth analysis of the smart contracts practice referring to such unsolved problems as accurate transference of the parties' will to the program code (translation of specific terms from the legal language into the smart contract program code), electronic identification of subjects – parties to the transaction and many other issues.

For citation

Varbanova, G. K. (2023). Legal Nature of Smart Contracts: Contract or Program Code? *Journal of Digital Technologies and Law, 1*(4), 1028–1041. https://doi.org/10.21202/jdtl.2023.44

Contents

Introduction

Smart contracts represent highly demanded tool necessary for modern law and economic. At the same time, despite its relevance and necessity there are still no clear regulation of smart contracts both on national and international level.

This study is intended to analyze the legal essence of smart contracts, their possible application in civil and commercial turnover. It is also aimed to provoke a broad discussion on the issues related to the manner of application of technologies and the need for their timely regulation. This study aims not only to give a legal definition of the term «smart contract», but to also reveal its characteristic features, interpreted in the light of the classical understanding of a contract, and from there to answer the question – Is smart contract, based on blockchain technology, is a contract itself?

In order to analyze the concept of a smart contract, we shall specify the features of blockchain technology and how it works, as well as what is the classical understanding of a contract underlying the civil law legal system. Only then we will be able to answer the question whether smart contracts may be considered a contract, does it give rise to rights and how shall the duties related thereto be performed. Last but not least, the features of smart contracts related to bringing the specific legal language into a program code will be analyzed.

1. Classic Contract Theory

The study of the legal nature of smart contracts requires an analysis of the contract theory and the manner in which contractual relations are created, developed and terminated. The etymology of the word «contract» reveals its main features. The word has a Latin origin «contractus» (noun), «contrahere» (verb) and means «to connect». A contract is often defined as a promise or group of promises that binds the parties in a civil transaction. This commitment is backed by state coercion, which is intended to ensure that the promise, the commitment in the contractual relationship, will be performed. Actions in Roman Law arose as a remedy for a wronged right. They are the procedural mechanism aimed at removing the consequences of the non-performe contract. A procedural opportunity for the parties, through the means of state coercion, to ensure the result that they pursued by entering into the contract.

At the beginning of the 19th century, the theory of autonomy of the will began to gain popularity. It is based on the understanding that contract as such is a consequence of the coordinated will of the parties to the legal transaction. Subjects are free to enter into contractual relations voluntarily, negotiating the parameters of the contract themselves as a counterpoint to obligations imposed by law or obligations arising from tort, asserted through the special sanction of the state. According to this theory, the role of the contract is to «facilitate the freedom of the parties to create their own private law». Although the theory of the autonomy of the will has certain deficiencies, it impacts the development of modern contract law and is expressed in the current legal norms – the principle of freedom of contract.

Private law relations and contract law in particular is the place where the principle of the autonomy of the human will is most clearly manifested. Subjects, upon mutual consent, in accordance with the principle of the autonomy of human will, are free to determine the content of the legal relationship they wish to enter into. Namely because the will of the parties is conclusive, the court – when interpreting the contracts – is obliged to look for their actual common will, and when interpreting the contract it shall be guided by it. The principle of the autonomy of the human will should not be considered absolute, which is why a number of legislations, including the Bulgarian one, have mitigated its application by introducing restrictions and applying other factors to protect both the interests of the parties and

the public interest. Thus, according to Article 9 of the Bulgarian Obligations and Contracts Act, the parties may freely determine the content of the contract, but this content shall not contradict the imperative legal provisions and good morals. Thus, the Supreme Court of Cassation of the Republic of Bulgaria, in its interpretive case law, defines good manners as moral norms to which the law has assigned legal significance, because the legal consequence of their violation is made equal to the conflict of the contract with the law. Good manners are not written, systematized and specified rules; they rather exist as general principles or originate from such, and the court monitors the compliance therewith ex officio. Therefore, either party is free to decide whether or not to enter into a specific contractual relationship, taking into account the imperative (mandatory) legal norms and good manners. Once an agreement is reached, the parties may decide what will be the content of the contract to be made (scope of rights and obligations) and when to conclude it. Parties can themselves choose whether and in what form to conclude the contract (Yossifova, 2019). Even tacitly expressed will can bind the parties, and the contract will be considered concluded unless the legislature has a requirement of form. The requirement of form is a requirement ad solemnitatem. The lack of form entails the nullity of the contract. Even if the parties have drafted a document, if it is not in the form prescribed by law, it will not produce the legal effect sought by the parties. Generally, the Bulgarian legislator adheres to the notion that most contracts are informal. Only when the objective is to guarantee legal certainty, the legislator has provided that certain contracts must be in writing or in a qualified form (notarized authentication or notarial deed). It should be noted that according to Bulgarian law, the written form requirement is considered complied with if an electronic document is generated containing a verbal statement, i.e. when the legislator requires certain contracts to be drafted in writing, it will be considered complied with if an electronic document that contains a verbal statement has been drawn up.

2. Blockchain and the concept of the smart contract

The idea of smart contracts is not new (Sala-Climent, 2021; Ferreira, 2021, Fiorentino & Bartolucci, 2021; Eenmaa-Dimitrieva & Schmidt-Kessen, 2019). The world of computer science and cryptography noticed it as early as 1996, when the computer engineer Nick Szabo presented his idea for self-executing program code. At the heart of Szabo's idea is a computer code where the will of the parties is implemented and which code executes itself when certain conditions occur so as to produce the outcome desired by the parties. The terms of the contract are written directly in code lines, i.e. the contract as such constitutes a program code. To better illustrate his idea, Szabo gives an example with a vending machine. The purchaser of a beverage from a vending machine has many implied consumer rights, and in practice the purchase of a beverage from a vending machine is an informal contract that, by means of a program code, provides each consumer with a selected

item for a specified price. Thus, the fact that a contract is represented only in a code, as in the case of smart contracts, does not constitute a particular obstacle to the conclusion of an informal contract, the execution of which is automated through a program code. Although revolutionary, Szabo's idea was ahead of its time because the technologies had not reached a level to allow for its mass application.

In 2008, Satoshi Nakamoto presented his idea for a decentralized blockchain network, and in 2014, Vitalik Buterin published Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, which revived the concept of self-executing program code (Zhou et al., 2020). A smart contract is an automated program code that is not in itself a technology for creating an artificial intelligence (Gallese, 2022). The self-execution of the smart contract is not related to automated data processing of data so as to make the most correct decision when certain situation arises. It involves automated execution – when event X occurs, an action Y is performed, without an option for the smart contract to assess, through data analysis, whether to proceed with execution or not. A smart contract is intended to reduce costs and skip the "trust" factor in contracting. Essentially, its objectives are speed, substantial cost reduction, avoiding intermediaries and overcoming the lack of trust between the parties. Execution of smart contracts is direct, without any additional action/ omission on behalf of the contracting parties being needed; it suffices that the condition preset in the program code occurs, and the consequences will occur immediately in the legal sphere of the parties. A major advantage, but also a disadvantage, of blockchain technology is that it does not allow any data modification. The block itself, and the block chain, is a cryptographic method of storing data in a decentralized environment. The smart contract is stored in the decentralized, blockchain ledger, which is why no separate device is needed for its storage, nor is it necessary for the parties thereto to keep a record on a local or other technical means (Compagnucci et al., 2021). Transactions in it are chronologically connected, allowing records to be traced from the last to the first block on the chain (genesis block). Once recorded in a block of the blockchain chain, it cannot be changed (altered) or deleted (Aleksieva et al., 2019), because each block of the blockchain chain has integrity, and each transaction is authenticated in time – each block of the chain contains a record of transactions and timestamp information of the proceeding block (Krumov & Atanasov, 2019). This actually ensures the chronological connectivity of the information in the blockchain and enables traceability back to the first genesis block. What does this mean? Deletion or alteration (modification) in the block would break the blockchain chain, which would affect the block verification process. Once the contract in the form of a smart contract is concluded, the will of the parties cannot be changed or altered, i.e. if subsequently their relationship undergoes a change, the parties will have to enter into a new smart contract, through which they will terminate the effect of the already existing one and rearrange their relationship. This, in turn, raises many questions to science and practice.

3. Legal language vs. program code

From the standpoint of science and practice, one of the underlying questions is how to transfer («translate») the specific terms from the legal language into the program code of the smart contract. When using smart contracts, we must account for the specific legal terms used in legal provisions and their correct implementation in the program code of the smart contract (Rizos, 2022). This is because, as stated, an alteration or deletion of the entry in the decentralized ledger is impossible, and the exact transfer of the will of the parties into a program code is of utmost significant, insofar as the program code must reflect the actual will of the parties. If the will of the parties is incorrectly transferred into the program code, the smart contract may self-execute, but its execution would not be the result intended by the parties. In such a situation, the only possible solution would be to materialize the actual will of the parties in a new record, in the form of a new smart contract, because the original record cannot be edited or deleted. The new entry is subject to whether the parties would agree to do so. It is possible that one of the parties has benefited from its incorrectly implemented will in the program code, and therefore prefers to preserve the consequences as they have occurred, although this is a result different from the one agreed between the parties. In this hypothesis, court intervention is necessary, which, by interpreting the will of the parties, would reveal what their actual will is, taking into account their pre-contractual relations. However, such an error in the will of the parties is also conceivable in classic contractual relations, which arise, develop and live their own life in the form of a conventional, written document.

Another material feature of smart contracts is that they are subject to the general rules of how the law regulates public relations in terms of the various types of transactions. When choosing certain contractual relations to be set forth in a smart contract, the parties must observe whether there is a requirement for contractual form, and whether this requirement is for its validity or for its proof. Thus, if a real estate is to be disposed of, the transaction will be subject to the general rules and in order for such transaction to be valid, it will have to be performed in accordance with the requirement for form - a notarial deed (according to the Bulgarian law). The execution of a transaction for disposition with real estate, in the form of a smart contract, will be null and void, as long as the requirement for a form – a notarial deed – has not been complied with. It is possible, in such a hypothesis, to think about the conversion of the smart contract and viewing it as a preliminary contract for the purchase and sale of real estate. Such a conversion depends on the particularities of the applicable law and on the interpretations given in binding case law. From the point of view of Bulgarian law, it is possible to apply conversion of the smart contract with subject-matter purchase and sale of real property, taking into account art. 3, paragraph 2 of the Electronic Document and Electronic Certification Services Act, setting forth that the written form of the smart contract would be deemed complied with only if the smart contract contains, in addition to program code, a verbal statement of the parties (Varbanova, 2020a).

4. Smart contract as a legal contract

From current legal framework standpoint, there is no impediment for the contractual relations for which there is no requirement for a form (including a qualified one) to be concluded in the form of a smart contract (Rühl, 2021). According to 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/EO[1] means any content stored in electronic form, in particular text or sound, visual or audiovisual recording. The list in the Regulation is not exhaustive. Quite logically, the legislator has considered that booming of technologies would result in the emergence of new technological solutions and the concept of an electronic document would have an even wider scope (Varbanova, 2020b). The regulation expressly binds the courts and obliges them to accept electronic documents in their court proceedings. The court cannot ignore the existence of the electronic document, although at first sight the electronic document cannot be perceived by the court as it would perceive the classic, written document. Analyzing Article 3, item 35 of the Regulation, we can conclude that the smart contract should be perceived as an electronic document, even though it exists in the form of a program code. Thus, in the example of a real estate transaction above, this property can be tokenized, but not for the purpose of selling, but for example only for the purpose of renting the property – a rental relationship. Lease contract is an informal contract. From this point of view, proving such contract would be much easier if it exists in the form of a smart contract and a tokenized real asset. The parameters of the rental relationship will be set forth in the smart contract – rental price, method of payment, term, etc. By combining IoT and blockchain technology, payment under the contract can be done automatically, while in the absence of receipt of the rental price into the owner's electronic wallet, the access to the dwelling can be automatically restricted by locking it using Internet of Things technological solutions. In the Internet of Things, end devices interact with each other through the global network – the Internet. The application of blockchain and IoT depends on the will of the parties and how that will would be implemented in the smart contract of the tokenized real asset.

Another problem that can arise with the use of smart contracts is that the case law is hard in responding to technological achievements. Courts often perceive as document only the conventional document materializing the will of the parties on paper, while the smart contract is a program code that exists as an entry in a decentralized ledger. This, however, cannot be an obstacle to respecting the will of the parties, who, especially in informal contractual relations, are free to choose how to conclude a contract and what technological solutions to use in this regard.

[1] 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. https://clck.ru/36r5fJ

Identification (Dimitrov et al., 2020) of the subjects – parties to the transaction, can also be an issue when using smart contracts based on blockchain technology. So long as there is no uniform legal framework regarding electronic identification, at this stage the solution of issues related to the identification of parties will be determined by the applicable law and the way in which the parties wish to benefit from the blockchain technology. Thus, when creating an electronic wallet, some providers of the service require the wallet owner to verify his personal data (Zahariev, 2021), including by providing a copy of an identity document in order to establish who is the person, who owns the relevant electronic wallet. It is essential that every single transaction from and to a given wallet is traceable and easily ascertainable.

In order to achieve the objectives of the contract, and also in view of the fact that its performance may depend on the occurrence of some event beyond the will of the parties, the technology allows the use of external sources – «oracles» (Bomprezzi, 2021). The oracle is an independent source of information that resides outside the smart contract blockchain (Basilan & Padilla, 2023). In the field of insurance law, the use of oracles would be essential when information is needed which is relevant to the insurance contract and the insured event occurring under it – temperature, natural disaster, etc. The application of oracles is also conceivable when blockchain technology and the smart contract are used to secure a claim (Gromova, 2018) – e.g., blocking a certain digital asset that can be released only upon provision of external information from an oracle, e.g., for a payment made on a claim secured by digital asset (Nascimento & Martins, 2022). A problem that could arise is when the oracle provides the wrong information and the smart contract executes itself in accordance with its embedded algorithm. In these cases, court intervention will be necessary, but court intervention will be required whenever one of the parties' defaults, and the smart contract actually eliminates such a possibility. Whenever the event embedded in the program code occurs, the smart contract executes the algorithm embedded in it, without such execution depending on the will of the parties.

Conclusions

Based on the analysis, we can define the Smart Contract – it is a program code where the parties have set in advance the conditions under which the contractual relationship between them is created, amended and terminated. The performance of the contract does not depend on an action or omission of the parties thereto, but rather on the occurrence of a pre-set condition (certain fact relevant to the parties) upon which the contract shall self-perform (self-executed). The will of the parties cannot be amended or replaced namely because of the specific manner of recording the smart contract in the decentralized ledger. Based on the analysis, we can conclude that certain types of contracts can be entered into in the form of a smart contract. When entering into a smart contract, the parties must comply

with the current legal framework, which may limit the performance of certain transactions in the form of a smart contract, especially when the legislator has set a requirement for form in entering into certain types of contracts. A serious challenge to legal science and practice is how to implement the will of the parties in the smart contract, with a correct understanding of legal concepts and their inclusion in the program code of the smart contract.

References

Aleksieva, V., Valchanov, H., & Huliyan, A. (2019). Application of Smart Contracts based on Ethereum Blockchain for the Purpose of Insurance Services. *2019 International Conference on Biomedical Innovations and Applications (BIA)* (pp. 1–4). https://doi.org/10.1109/BIA48344.2019.8967468

Basilan, M. L. J. C., & Padilla, M. (2023). Assessment of teaching English Language Skills: Input to Digitized *Activities for campus journalism advisers. International Multidisciplinary Research Journal*, *4*(4), 118–130. https://doi.org/10.54476/ioer-imrj/245694

Bomprezzi, Ch. (2021). Implications of Blockchain-Based Smart Contracts on Contract Law. *Luxemburger Juristische Studien – Luxembourg Legal Studies*, *23*. https://doi.org/10.5771/9783748930068

Compagnucci, M. C., Fenwick, M., & Wrbka, S. (2021). The Uncertain Future of Smart Contracts. *Smart Contracts*, *12*, 11–12. https://doi.org/10.5040/9781509937059.ch-009

Dimitrov G., Petrivskyi V., Bychkova O., & Garvanova, M. (2020). Information technology for big data sensor networks stability estimation. *Information & Security*, *47*(1), 141–154. https://doi.org/10.11610/isij.4710

Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M.-J. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law & Security Review*, *35*(1), 69–88. https://doi.org/10.1016/j.clsr.2018.09.003

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution? *Telecommunications Policy*, *45*(2), 102081. https://doi.org/10.1016/j.telpol.2020.102081

Fiorentino S., & Bartolucci S. (2021). Blockchain-based smart contracts as new governance tools for the sharing economy. *Cities*, *117*, 103325. https://doi.org/10.1016/j.cities.2021.103325

Gallese, Ch. (2022). *Predictive Justice in Light of the New AI Act Proposal*. https://doi.org/10.2139/ssrn.4286023

Gromova, E. (2018). Smart contracts in Russia: an attempt to define the legal nature of smart contracts. *Law and Digital Economy*, *2*, 31–33. https://doi.org/10.17803/2618-8198.2018.02.2.031-033

Krumov, K., & Atanasov, A. (2019). The peculiarities of Blockchain technology. *Journal of Informatics and Innovative Technologies*, *1*, 3–6.

Nascimento, S. N. & Martins, D. G. D. (2022). Smart Contracts: Security Issues and Further Development in Brazil. *International Journal of Law in Changing World*, *1*(2), 26–45. https://doi.org/10.54934/ijlcw.v1i2.22

Rizos, E. (2022). A contract law approach for the treatment of smart contracts' 'bugs'. *European Review of Private Law*, *30*(5), 775–802. https://doi.org/10.54648/erpl2022037

Rühl, G. (2021). Smart (legal) contracts, or: Which (contract) law for smart contracts? *Blockchain, Law and Governance*, *8*, 159–180. https://doi.org/10.1007/978-3-030-52722-8_11

Sala-Climent, M. T. (2021). Smart contracts – technological, business and legal perspectives. *European Review of Contract Law*, *17*(4), 385–389. https://doi.org/10.1515/ercl-2021-2033

Varbanova, G. (2020a). *Legal regime of electronic documents*. Dangrafik, Varna.

Varbanova, G. (2020b). Smart contract and challenges to law. In *The law and the business in the contemporary society: Conference Proceedings of the 3rd National Scientific Conference* (pp. 359–364). https://doi.org/10.36997/lbcs2020.359

Yossifova, T. (2019). *Effect of Contracts Vis-à-vis Individuals*. Sibi, Sofia.

Zahariev, M. (2021). *Protection of personal data during video surveillance, Intellectual property in the new (ab) normal*. Sofia, AzBuki.

Zhou, Z., Li, R., Cao, Y., Zheng, L., & Xiao, H. (2020). Dynamic performance evaluation of blockchain technologies. *IEEE Access*, *8*, 217762–217772. https://doi.org/10.1109/access.2020.3040875

Author information

Gergana Varbanova – PhD, Assistant Professor at the Department of Legal Studies, University of National and World Economy, Arbitrator of the Arbitration Court of the BIA
Address: 10 Drin Street, Varna, Bulgaria
E-mail: gergana@varbanova.bg
ORCID ID: https://orcid.org/0000-0001-8122-4353
WoS Researcher ID: https://www.webofscience.com/wos/author/record/37781549
Google Scholar ID: https://scholar.google.com/citations?user=02-0uFYAAAAJ

Conflict of interest

The author is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – May 25, 2023
Date of approval – October 7, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:347.45/.47
EDN: https://elibrary.ru/igaziz
DOI: https://doi.org/10.21202/jdtl.2023.44

Правовая природа смарт-контрактов: договор или программный код?

Гергана Варбанова

Университет национального и мирового хозяйства;
Арбитражный суд BIA
Варна, Болгария

Ключевые слова

блокчейн,
гражданское право,
договор,
договорное право,
информационные технологии,
коммерческое право,
право,
программный код,
смарт-контракт,
цифровые технологии

Аннотация

Цель: цифровая экономика и договорные отношения, обусловленные стремительным изменением технологий, определяют трансформацию права и развитие законодательства в направлениях его адаптации к перспективам распространения и применения смарт-контрактов в гражданском и коммерческом обороте, в связи с чем нацеленность исследования на определение юридической сущности смарт-контрактов становится основополагающим этапом на пути к выработке своевременного и четкого их регулирования.

Методы: в основу исследования положена методология формально-юридического и сравнительно-правового анализа, позволяющая сопоставить нормы действующего болгарского законодательства и наднациональных источников права, а также выявить характерные черты смарт-контрактов как востребованных инструментов, необходимых для современного права и экономики, и сопоставить их с классическим пониманием контрактов, в сравнении с которым можно более точно понять и определить природу смарт-контрактов.

Результаты: определено, что смарт-контракт является программным кодом, в котором стороны заранее установили условия, при которых договорные отношения между ними создаются, изменяются и прекращаются; доказано, что исполнение контракта зависит не от действия или бездействия его сторон, а скорее от наступления заранее установленного условия (определенного факта, имеющего отношение к сторонам), при котором контракт должен самоисполняться; обосновано, что воля сторон не может быть изменена или заменена именно из-за особого способа записи смарт-контракта в децентрализованном реестре; выявлено, что основополагающей остается проблема передачи воли с юридического языка в программный код смарт-контракта – если воля сторон неправильно передана в программный код, смарт-контракт может самоисполниться, но его исполнение не будет тем результатом, на который рассчитывали стороны.

Научная новизна: проведенный анализ позволил сравнить современное национальное (болгарское) законодательство и наднациональное (европейское) право, выявив нечеткость регулирования смарт-контрактов как на национальном, так и на международном уровне, определив ряд нуждающихся в научной и правовой интерпретации вопросов о правовой природе смарт-контрактов в контексте концепции самоисполняющегося программного кода.

Практическая значимость: исследование может послужить основой для дальнейшего развития законодательства в направлениях его адаптации к перспективам распространения и применения смарт-контрактов в гражданском и коммерческом обороте, а также для углубленного анализа практики применения смарт-контрактов с точки зрения имеющихся неразрешенных проблем точной передачи воли сторон в программный код (перевода конкретных терминов с юридического языка в программный код смарт-контракта), электронной идентификации субъектов – сторон транзакции и многих других.

Для цитирования

Варбанова, Г. (2023). Правовая природа смарт-контрактов: договор или программный код? *Journal of Digital Technologies and Law*, *1*(4), 1028–1041. https://doi.org/10.21202/jdtl.2023.44

Список литературы

Aleksieva, V., Valchanov, H., & Huliyan, A. (2019). Application of Smart Contracts based on Ethereum Blockchain for the Purpose of Insurance Services. *2019 International Conference on Biomedical Innovations and Applications (BIA)* (pp. 1–4). https://doi.org/10.1109/BIA48344.2019.8967468

Basilan, M. L. J. C., & Padilla, M. (2023). Assessment of teaching English Language Skills: Input to Digitized *Activities for campus journalism advisers. International Multidisciplinary Research Journal*, *4*(4), 118–130. https://doi.org/10.54476/ioer-imrj/245694

Bomprezzi, Ch. (2021). Implications of Blockchain-Based Smart Contracts on Contract Law. *Luxemburger Juristische Studien – Luxembourg Legal Studies*, *23*. https://doi.org/10.5771/9783748930068

Compagnucci, M. C., Fenwick, M., & Wrbka, S. (2021). The Uncertain Future of Smart Contracts. *Smart Contracts*, *12*, 11–12. https://doi.org/10.5040/9781509937059.ch-009

Dimitrov G., Petrivskyi V., Bychkova O., & Garvanova, M. (2020). Information technology for big data sensor networks stability estimation. *Information & Security*, *47*(1), 141–154. https://doi.org/10.11610/isij.4710

Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M.-J. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law & Security Review*, *35*(1), 69–88. https://doi.org/10.1016/j.clsr.2018.09.003

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution? *Telecommunications Policy*, *45*(2), 102081. https://doi.org/10.1016/j.telpol.2020.102081

Fiorentino S., & Bartolucci S. (2021). Blockchain-based smart contracts as new governance tools for the sharing economy. *Cities*, *117*, 103325. https://doi.org/10.1016/j.cities.2021.103325

Gallese, Ch. (2022). *Predictive Justice in Light of the New AI Act Proposal*. https://doi.org/10.2139/ssrn.4286023

Gromova, E. (2018). Smart contracts in Russia: an attempt to define the legal nature of smart contracts. *Law and Digital Economy*, *2*, 31–33. https://doi.org/10.17803/2618-8198.2018.02.2.031-033

Krumov, K., & Atanasov, A. (2019). The peculiarities of Blockchain technology. *Journal of Informatics and Innovative Technologies*, *1*, 3–6.

Nascimento, S. N. & Martins, D. G. D. (2022). Smart Contracts: Security Issues and Further Development in Brazil. *International Journal of Law in Changing World*, *1*(2), 26–45. https://doi.org/10.54934/ijlcw.v1i2.22

Rizos, E. (2022). A contract law approach for the treatment of smart contracts' 'bugs'. *European Review of Private Law*, *30*(5), 775–802. https://doi.org/10.54648/erpl2022037

Rühl, G. (2021). Smart (legal) contracts, or: Which (contract) law for smart contracts? *Blockchain, Law and Governance*, *8*, 159–180. https://doi.org/10.1007/978-3-030-52722-8_11

Sala-Climent, M. T. (2021). Smart contracts – technological, business and legal perspectives. *European Review of Contract Law*, *17*(4), 385–389. https://doi.org/10.1515/ercl-2021-2033

Varbanova, G. (2020a). *Legal regime of electronic documents*. Dangrafik, Varna.

Varbanova, G. (2020b). Smart contract and challenges to law. In *The law and the business in the contemporary society: Conference Proceedings of the 3rd National Scientific Conference* (pp. 359–364). https://doi.org/10.36997/lbcs2020.359

Yossifova, T. (2019). *Effect of Contracts Vis-à-vis Individuals*. Sibi, Sofia.

Zahariev, M. (2021). *Protection of personal data during video surveillance, Intellectual property in the new (ab) normal*. Sofia, AzBuki.

Zhou, Z., Li, R., Cao, Y., Zheng, L., & Xiao, H. (2020). Dynamic performance evaluation of blockchain technologies. *IEEE Access*, *8*, 217762–217772. https://doi.org/10.1109/access.2020.3040875

Информация об авторе

Варбанова Гергана – PhD, ассистент кафедры правоведения, Университет национального и мирового хозяйства, арбитр Арбитражного суда BIA
Адрес: Болгария, г. Варна, ул. Дрин, 10
E-mail: gergana@varbanova.bg
ORCID ID: https://orcid.org/0000-0001-8122-4353
WoS Researcher ID: https://www.webofscience.com/wos/author/record/37781549
Google Scholar ID: https://scholar.google.com/citations?user=02-0uFYAAAAJ

Конфликт интересов

Автор является членом редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.27.41 / Сделки
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 25 мая 2023 г.
Дата одобрения после рецензирования – 7 октября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.45

Smart Contracts and International Trade: European Legal Strategies for Managing Challenges

Tharika Dishani Lamappulage Donn

University of Greenwich
London, United Kingdom

Keywords

algorithmic code,
blockchain technology,
computer software,
digital agreement,
digital technologies,
digitalization,
electronic form,
international trade,
law,
smart contract

Abstract

Objective: The automation inherent in smart contracts makes them an attractive tool for global trade applications, especially for the automation of transactions. The prospects foreseeable will significantly impact international economic relations and the transformation of international trade rules. This fact determines the study objective – to identify the possibilities of transforming the said rules and the political and legal strategies adopted by European countries to implement smart contracts in international trade.

Methods: the study, devoted to the current international trade regulation in the context of contracts digitalization and spread of smart contracts, uses a combination of formal-legal and comparative-legal methods. They allow researching the international trade rules, analyzing and comparing the UK and the EU political and legal positions on the smart contracts introduction in international trade, as well as predicting the legal consequences of using smart contracts in international trade.

Results: the research shows that the proliferation of smart contracts has significant implications for international trade and its regulation. Smart contracts have numerous advantages, such as increased efficiency, reduced costs, and wide availability. However, they may lead to legal challenges when harmonizing traditional legal principles with the digital

environment, in particular concerning the authentication of subjects, enforceability under specific circumstances of a case, and jurisdictional issues.

Scientific novelty: the current literature on the transformation of international trade regulation in the context of digitalization processes and the spread of smart contracts is complemented by the results of a comparative analysis of the legal positions existing in the European legal space and developed on the basis of problems, lessons and achievements in the smart contracts implementation in international trade.

Practical significance: understanding the legal implications of smart contracts is important for businesses involved in international trade. The study provides insights into the UK and the EU legal positions from which guidance can be provided to companies navigating the digital landscape. Policymakers can also benefit from the findings when developing appropriate legal acts to balance the benefits of smart contracts with the need for legal certainty and protection in international trade.

For citation

Lamappulage Donn, T. D. (2023). Smart Contracts and International Trade: European Legal Strategies for Managing Challenges. *Journal of Digital Technologies and Law, 1*(4), 1042–1057. https://doi.org/10.21202/jdtl.2023.45

Content

Introduction

Smart contracts are digital agreements that can be autonomously executed, enabling the corresponding parties to transfer digital and physical assets or anything of value between themselves in an open and conflict-free way (Hewa et al., 2021). American computer scientist Nick Szabo, designer of the digital currency Bit Gold, defined «smart contracts» as «computerized transaction protocols that execute terms of a contract» in 1998[1]. Satoshi Nakamoto also has planted the idea of a smart contract in his 2008 publication, Bitcoin: A Peer-to-Peer Electronic Cash System (Nakamoto, 2008). The number of bitcoins in circulation and the authority to create and move Bitcoins are monitored and controlled by a distributed database that runs on smart contract software. Similar to how vending machines have replaced human vendors, smart contracts have the potential to make intermediaries obsolete across a variety of sectors, as explained by Nick Szabo.

An individual who needs to finalise a complex transaction involving a substantial amount of money would typically seek the advice of a lawyer or notary, pay said professional, and then wait while the task was completed and the contract's conditions were met (Vatiero, 2023). Before the lawyer verifies that all paperwork has been correctly performed, he will not get access to the funds or the property. Simply by placing a bitcoin on the ledger, it can immediately obtain the deed, contract, products, driver's license, or whatever else is promised by the smart contract. Smart contracts introduce an extra software layer between consumers and blockchain storage (Ferreira, 2021). Smart contracts execute the logic necessary to provide a complicated service in reaction to demands from customers. This includes things like managing states, enforcing governance, and checking identities. Smart contracts allow users to store and access data from blockchain storage without the need to perform searches. To instead reach the core blockchain storage structures, smart contracts provide a computer interface (Bandara et al., 2019).

For centuries, the United Kingdom has maintained a solid system of law and is among the countries that are currently investigating and implementing smart contracts. In November 2021, Dominic Raab MP, who holds the positions of Lord Chancellor and Secretary of State for Justice, delivered a proposal for Smart legal contracts Advice to Government, which is regarded as a progressive measure in the ongoing process[2]. European Union countries have also taken smart measures related to smart contracts in recent years. This paper is focusing on the implementation process of smart contracts within the UK and in EU while analysing the impact of them on international trade regulations in the context of digitalisation. The study also aims to evaluate the legal framework of the UK and the EU with respect to smart contracts. It seeks to assess the compatibility of the legal framework with smart

1 Zapotochnyi, A. (2022, October 19). What are smart contracts?. Blockgeeks. https://clck.ru/36kyjY

2 The Law Commission. (2021). Smart legal contracts Advice to Government. https://goo.su/FohUZ

contracts and examine the challenges and achievements encountered in promoting smart contracts in international trade (Zhang et al., 2023).

Black letter research, also known as doctrinal research, is an approach that primarily involves the analysis of legal sources, such as statutes, case law, and legal commentary (Fatima, 2023). A comprehensive analysis of the existing legal framework for smart contracts in the UK and EU had conducted utilising above research method. The study has analysed relevant documents, such as academic literature, government reports, and industry publications, to gain insights into the legal and regulatory framework, use cases, benefits, challenges, and lessons learned from the UK's experience with smart contracts. The analysis had focused on identifying any legal challenges facing the adoption of smart contracts in the UK and any legal solutions that can be implemented to address these challenges.

Qualitative research which is an approach that involves exploring and understanding the meanings, experiences, and perspectives of individuals or groups through methods such as observations, and document analysis also had used as a methodology in this paper.

1. How smart contracts work?

There are several kinds of smart contracts such as smart legal contracts and Ricardian contracts. Smart contracts can be used to facilitate a wide variety of business processes, asset exchanges, and other kinds of deals, the details of which are determined by the parties involved based on their level of cooperation and their desired outcomes (Ji et al., 2023; Ante, 2021). An occurrence or situation, such as a shift in a financial market indicator or a user's GPS coordinates, can initiate a smart contract either by the parties to the contract or on their behalf (Gunay & Kaskaloglu, 2022; Wang et al., 2023a). When the requirements of a computer software are met, the programme runs automatically without any further input from the programmer. Communication between the participants to a smart contract can be authenticated and transmitted securely due to encryption (Kirli et al., 2022). Ethereum is currently the most popular tool for creating and implementing smart contracts, but other blockchain-based cryptocurrencies like EOS, Neo, Tezos, Tron, Polkadot, and Algorand can do the same thing (Sathiyamurthy & Kodavali, 2023; Liu et al., 2023). Each network server will update its own record after smart contracts have been executed to reflect the operational state of the network at that time. The document can no longer be edited after it has been uploaded to the blockchain network and verified. The trustworthiness of international trade contracts can be effectively addressed by employing the immutable and distributed properties of the blockchain (Pishdad-Bozorgi & Han Yoon, 2022).

The Ethereum Virtual Machine (EVM) is accountable for the administration of smart contracts on the Ethereum blockchain within the Ethereum platform (Liu et al., 2022; Wang et al., 2023b). Prior to initiating any compiled smart contract on specific blockchains, it is mandatory to make payment of a transaction fee known as the 'gas' fee. In regards to operational procedures, a complex smart contract will incur a greater gas cost for its execution. The utilisation of gas is implemented to safeguard the Ethereum Virtual Machine

from potential overloading caused by smart contracts that are either excessively intricate or excessively numerous (Eenmaa-Dimitrieva & Schmidt-Kessen, 2019). At its fundamental level, gas can be conceptualised as the propulsive agent that propels the smart contracts of Ethereum. Insufficient gas reserves would impede the network's ability to carry out transactions. Each transaction is associated with a gas fee, and the initiation of transactions is contingent upon the distribution of contracts throughout the network. The execution of Ethereum transactions requires a significant number of computational resources. The computation required for a transaction determines the gas fee charged[3].

2. Background of smart contracts in UK and EU

2.1. Approach of the UK

The UK government's «Innovate UK» programme began selling Blockchain as a service (BaaS) on August 3, 2016. HM Revenue and Customs is evaluating the adoption of blockchain technology, in addition to exploring various other technical alternatives, for the purpose of enhancing tax and customs as well as excise systems. In May 2016, the Parliamentary Office of Science and Technology (POST) generated a concise report on Financial Technology, with particular emphasis on four nascent domains, one of which was Distributed Ledger Technology (DLT). In January 2018, POST released a document titled «topics of interest», wherein distributed ledger technologies (DLTs) were identified as an area requiring further research. A trial has been conducted by the Department for Work and Pensions in collaboration with GovCoin to explore the potential of blockchain technology in facilitating welfare payments (Hughes et al., 2018). The UK Jurisdiction Taskforce (UKJT) reached a conclusion in 2019 that the enforceability of smart contracts is contingent upon the specific circumstances of the case. The Law Commission had been assigned the task of assessing the reliability of the existing legal and legislative framework in light of the requirement to manage smart legal contracts, highlighting any uncertainties, and/or suggesting new and/or updated laws if necessary (Ferro et al., 2023). Despite these legislative efforts, however, there is still a dearth of studies evaluating the success of these measures in implementing smart contracts in the UK (Blaszczyk, 2023).

2.2. Approach of the EU

On April 11, 2018, twenty-two countries across Europe joined forces to establish a new body known as the European Blockchain Partnership. This coalition of nations includes the Netherlands, Germany, France, Norway, and Spain, amongst others. Mariya Gabriel, the European Commissioner for Digital Economy and Society, stated that Blockchain

[3] Frankenfield, J. (2022, September 27). Gas (Ethereum): How Gas Fees Work on the Ethereum Blockchain. Investopedia. https://clck.ru/36kytz

is an excellent opportunity for Europe and member states to reconsider their information systems, to encourage confidence in users and the safety of personal data, to help develop new business opportunities and to establish emerging fields of leadership, which will benefit the public, public services, and business entities.

The concept of an "E-Resident" was first introduced in Estonia in 2014. People from all over the world participated in the digital programme by becoming digital residents and registering companies in Estonia. Confronting this situation, the blockchain movement emerged, which promotes the decentralisation of services. Combining Estonia's E-resident programme with blockchain technology is a smart move. E-Estonia is an Ethereum-based programme at the moment. Official preparations for an ICO in Estonia are still in the works. The ESTcoin was created to add a new dimension and convenience to the E-resident scheme. Improvements are on the horizon for the E-resident Ecosystem (Kim, 2023).

The European Parliament approved new data controls for inclusion in a bigger bill on data privacy on March 14th, 2023. The bill is intended to handle data privacy without stifling innovation (Perez & Zeadally, 2023). All smart contracts must now have a «kill switch,» per a new provision in the law known as the Data Act. In the event of a security breach, administrators of IT frequently use a «kill switch» method to immediately disable a system. In the event of a critical flaw or breach, a kill switch in a smart contract programme can either immediately terminate the contract or stop, patch, and re-release it[4].

3. Legal background for international trade in UK and EU

3.1. International trade policy of the UK

The prosperity of both the UK's economy and the global economy is contingent upon the presence of unrestricted and impartial trade. Consequently, the escalation of wages leads to an increase in the accessibility of a wider spectrum of reasonably priced commodities and amenities, thereby resulting in augmented household earnings, especially for the most susceptible segments of the populace. More than 50 % of the UK's Gross Domestic Product is comprised of its international trade activities. The UK formally departed from the EU on January 31, 2020, following a referendum held in June 2016. The European Union (Withdrawal) Act 2018 was implemented by the UK to assimilate EU laws and regulations into the domestic legal framework of the country. This was done by substituting references to EU organizations, laws, and regulations with corresponding UK references, with the aim of ensuring continuity in legal coverage and processes and avoiding any potential disruptions. Following the events of January 1, 2021, it can be observed that the legal and regulatory frameworks of both the UK and the EU were almost similar. However, it is noteworthy that the UK now possesses the autonomy to modify its laws and regulations without seeking

[4] Shamai, S. (2023, March 29). The EU's Smart Contract 'Kill Switch' Mandate Won't Kill Crypto. Coindesk. https://clck.ru/36kywE

consultation from the EU. The UK and EU have recently reached an agreement on the UK-EU Trade and Cooperation Agreement (TCA), which came into effect on January 1, 2021. This new trade deal ensures that both parties can continue to access each other's markets without incurring tariffs or quotas, while also allowing for independent regulatory frameworks for the UK and EU (Buigut & Kapar, 2023). As per the provisions of the TCA, it is permissible for either party to endeavour to modify the agreement by altering market access obligations in the event of significant trade implications arising due to variations in domestic regulatory frameworks[5].

The implementation of the UNCITRAL Model Law on Cross-Border Insolvency in the UK has been carried out through the Cross-Border Insolvency Regulations 2006. The UK's early consideration of the implementation of these measures will serve as a clear indication of its continued dedication to mutual collaboration and adherence to global standards. Smart contracts are legally valid under the Convention on the International Sale of Goods, as they satisfy the offer and acceptance criteria specified in Articles 14 and 18. Nevertheless, it is noteworthy that the UK persists as one of the few industrialised countries globally that has yet to implement the CISG. There exist several factors contributing to this phenomenon, such as the fact that the CISG exhibits a greater inclination towards civil law, a lack of sufficient motivation on the part of businesses to advocate for its ratification, and the potential for a reduction in the significance of London as a centre for commercial arbitration (Hoekstra, 2021).

3.2. International trade policy of the EU

The trade and investment policy of the EU is responsible for managing its trade and investment relations with countries outside of the EU. It is the responsibility of the EU, not the national administrations of individual member countries, to conduct trade with countries outside the EU. The EU institutions are responsible for the creation of legislation pertaining to trade affairs, as well as engaging in the negotiation and finalisation of global trade accords. The EU adheres to the fundamental principles of the World Trade Organization. During June of 2018, amidst increasing trade tensions on a global scale, the European Council emphasised the importance of safeguarding and enhancing the multilateral system that operates based on established rules. The EU has conveyed its willingness to enhance the operational efficiency of the World Trade Organization in collaboration with other nations that share similar views. Trade agreements are intricate in nature as they comprise of legal documents that encompass a broad spectrum of activities, ranging from agriculture to intellectual property. However, they exhibit a multitude of underlying principles that are common[6].

5 GOV.UK. (2018). UK trade policy: A guide to new trade legislation. https://clck.ru/ZBrtd

6 European Commission. Making Trade Policy. https://clck.ru/36kz2m

4. How digitalisation of Contracts in UK and EU

4.1. Legal Progress of the UK

The Thirteenth Programme of Law Reform requested the Law Commission to undertake research and analysis on the subject of smart legal contracts, as per the direction of the Lord Chancellor. The legal statement on crypto assets and smart contracts was published by the UK Jurisdiction Taskforce ("UKJT") in November 2019. As per the UKJT Legal Statement, it has been determined that smart contracts possess the potential to generate legally binding obligations that can be enforced in accordance with their respective terms. Subsequently, the Ministry of Justice has requested the Law Commission conduct a comprehensive examination of the existing legal framework concerning smart legal contracts. Therefore, the commission has carried out further analysis aimed at elucidating any ambiguities or deficiencies in the current legislation and determining any additional research that may be necessary at present or in the future.

In cases where contractual disagreements arise, the courts will rely on a particular publication that provides an interpretation of the contracts in question. This publication stipulates that the courts will assess the meaning of the programming language used in the contract from the perspective of a rational programmer, taking into account all relevant contextual information that was available to the parties involved at the time the contract was formed. According to the perspective of the Law Commission, it is imperative to subject even intelligent legal contracts that are composed entirely of code to interpretation, given the potential for a discrepancy between the intended meaning of the code and its actual execution. This is due to the distinction between the semantic interpretation of the code and its practical implementation. The incorporation of code within the interpretive framework may potentially result in interpretational challenges. According to the Law Commission, it is recommended that the assessment utilised should be a variant of the conventional test, wherein the interpretation of a coded term would be based on the comprehension and awareness of an individual with expertise in the relevant field (Durovic & Willett, 2023). According to the Commission, this aligns with the prevailing method of construing contracts.

The importance of certainty from a legal standpoint cannot be overstated. It is noteworthy that English law is acknowledged as having the capacity to incorporate smart contracts. This implies that in cases where a smart contract is subject to English law, the parties involved in the computerised global trade agreement should feel reassured. Furthermore, the report by the Law Commission presents factors that contracting parties should take into account, which will be especially relevant to individuals working in the realm of Decentralised Finance.

4.2. Legal Progress of the EU

Legislation pertaining to smart contracts and the internet of things was adopted by the European Parliament on March 14th of 2023, as part of the Data Act. The legislation was approved by a significant majority of five hundred votes in favour and twenty-three against,

with the objective of promoting the growth of business models to foster the emergence of novel industries and employment opportunities. The Data Act's Article 30 comprises stipulations concerning the fundamental prerequisites concerning smart contracts for the purpose of data sharing (Casolari et al., 2023). Commencing in 2024, corporations must comply with the newly established regulations in order to offer their services or merchandise to consumers located within the EU. The Act's content was adopted by the European Parliament and is currently slated for trialogue. Upon approval of the Act, a nationwide implementation period of 12 months will follow.

The implementation of the Data Act necessitates the establishment of mechanisms that can effectively cease the ongoing execution of transactions. These mechanisms may include internal functions that facilitate the resetting of the contract or provide instructions for its termination. It is imperative to establish a precise delineation of the circumstances that warrant the resetting or cessation of a smart contract. Within the realm of information technology, administrators frequently employ the kill switch mechanism as a means of terminating a device, network, or software in response to a security threat (Philip & Saravanaguru, 2022). Within the context of a smart contract environment, a kill switch has the capability to either terminate the contract or initiate a cessation, repair, and subsequent reissue of the contract in the event of a significant vulnerability or violation (Chu et al., 2023).

The Data Act represents a crucial initiative aimed at enhancing the accessibility of data in accordance with the principles and regulations of the EU. It constitutes a fundamental component of the European data strategy. This will significantly contribute to the objective of digital transformation outlined in the Digital Decade initiative. The evaluation of adherence to the fundamental prerequisites will be conducted by the smart contract vendor or provider. Subsequently, they will be required to furnish an EU declaration of conformity and assume accountability for conformity with the essential requirements. The definition of «responsible» in this particular context remains ambiguous, and it is uncertain whether users of the smart contract may face any civil liability. In the event that a supplier fails to furnish a smart contract that adheres to regulatory standards, the repercussions will be ascertained in accordance with the governing laws of the relevant member state.

4.3. The view of WTO

WTO has published several reports on smart contracts and related technologies, and according to those reports, they are of the opinion that the inherent automation of smart contracts renders them a compelling instrument for employment in the realm of global commerce, specifically for the purpose of automating transactions. The utilisation of smart contracts gives rise to legal concerns that necessitate careful consideration, particularly with respect to matters of enforcement and liability that may require attention in the event of erroneous coding of the contract (Papadouli & Papakonstantinou, 2023). Furthermore, smart contracts are software applications that, akin to any code, may harbour inadvertent errors. 'The blockchain ecosystem' is susceptible to security vulnerabilities primarily in the layer of smart contracts as well as the user interface, which may include

devices such as mobile phones, tablets, or computers utilised for internet access[7]. WCO/WTO Study Report on Disruptive Technologies also shows how can the smart contracts utilise in international trade and in the shipping process[8].

Therefore, it is clear that the international trade organisation is on the process of considering to adapt smart contract in international trade which may be an encouragement to the buyers and sellers to engage more in this technology to save the time and money.

Conclusion

Smart contracts are made up of lines of code that automatically carry out all or parts of an agreement. Even smart contracts written entirely in code can be valid under the CISG because they satisfy the Convention's offer and acceptance conditions in Articles 14 and 18.

The UK and the EU are currently taking a progressive approach to smart contracts. The UK is trying to adapt an existing legal framework to regulate smart contracts, and conflicts arise pertaining to those, while the EU is trying to regulate the execution of legal contracts with new legislation. WTO is also continuing the feasibility studies regarding smart contracts and other related technologies. Therefore, it can be concluded that the international trade rules will not be much affected by the digitalization of the contracts as per the current situation. However, as smart contracts are still an emerging technology, there can be a need for new legislation to address the novel issues that might arise in the future.

References

Ante, L. (2021). Smart contracts on the blockchain – A bibliometric analysis and review. *Telematics and Informatics*, *57*, 101519. https://doi.org/10.1016/j.tele.2020.101519

Bandara, E., Ng, W. K., Ranasinghe, N., & De Zoysa, K. (2019). Aplos: Smart Contracts made smart. In J. F. Ashish, Gh. R. Oliveira, P. L. Zhou (Eds.), *Communications in Computer and Information Science* (pp. 431–445). https://doi.org/10.1007/978-981-15-2777-7_35

Blaszczyk, M. (2023). *Smart contracts, Lex cryptographia, and transnational contract theory*. SSRN. https://doi.org/10.2139/ssrn.4319654

Buigut, S., & Kapar, B. (2023). How did Brexit impact EU trade? Evidence from real data. *The World Economy*, *46*(6), 1566–1581. https://doi.org/10.1111/twec.13419

Casolari, F., Taddeo, M., Turillazzi, A., & Floridi, L. (2023). How to improve smart contracts in the European Union Data Act. *Digital Society*, *2*(1). https://doi.org/10.1007/s44206-023-00038-2

Chu, H., Zhang, P., Dong, H., Xiao, Y., Shunhui, J., & Wenrui, L. (2023). A survey on smart contract vulnerabilities: Data sources, detection and repair. *Information and Software Technology*, *159*(107221). https://doi.org/10.1016/j.infsof.2023.107221

Durovic, M., & Willett, C. (2023). A legal framework for using smart contracts in Consumer Contracts: Machines as servants, not masters. *The Modern Law Review*. https://doi.org/10.1111/1468-2230.12817

7 Ganne, E. (2018). Can Blockchain Revolutionize International Trade? https://clck.ru/36kz6N

8 WTO and World Customs Organization. WCO/WTO Study Report on Disruptive Technologies. (2022). https://clck.ru/36kzCD

Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law & Security Review*, *35*(1), 69–88. https://doi.org/10.1016/j.clsr.2018.09.003

Fatima, S. (2023). Employability of a Research Method and Methodology in a Socio-Legal Study. *Global Social Sciences Review*, *VIII*(I), 341–351. https://doi.org/10.31703/gssr.2023(VIII-I).31

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution? *Telecommunications Policy*, *45*(2), 102081. https://doi.org/10.1016/j.telpol.2020.102081

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Corrias, G., Moncada, R., Cavallaro, A., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, *4*(3), 100142. https://doi.org/10.1016/j.bcra.2023.100142

Gunay, S., & Kaskaloglu, K. (2022). Does utilizing smart contracts induce a financial connectedness between Ethereum and non-fungible tokens? *Research in International Business and Finance*, *63*, 101773. https://doi.org/10.1016/j.ribaf.2022.101773

Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, *177*, 102857. https://doi.org/10.1016/j.jnca.2020.102857

Hoekstra, J. (2021). Political barriers in the ratification of international commercial law conventions. *Uniform Law Review*, *26*(1), 43–66. https://doi.org/10.1093/ulr/unab003

Hughes, E., Graham, L., Rowley, L., & Lowe, R. (2018, July 1). Unlocking blockchain: Embracing new technologies to drive efficiency and empower the citizen. *The Journal of The British Blockchain Association*, *1*(1), 63–72. https://doaj.org/article/6b966411b40746de873b99f25546bfca

Ji, B., Zhang, M., Xing, L., Li, X., Li, Ch., Han, C., & Wen, H. (2023). Research on optimal intelligent routing algorithm for IoV with machine learning and smart contract. *Digital Communications and Networks*, *9*(1), 47–55. https://doi.org/10.1016/j.dcan.2022.06.012

Kim, N. (2023). National ID for public purpose. *Georgetown Law Technology Review*, *7*(2). https://clck.ru/36kzR3

Kirli, D., Couraud, B., Robu, V., & Salgado-Bravo, M. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, *158*, 112013. https://doi.org/10.1016/j.rser.2021.112013

Liu, L., Wei-Tek, T., Zakirulm A., Hao, P., & Mingsheng, L. (2022). Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum. *Future Generation Computer Systems*, *128*, 158–166. https://doi.org/10.1016/j.future.2021.08.023

Liu, H., Fan, Y., Feng, L., & Wei, Z. (2023). Vulnerable smart contract function locating based on Multi-Relational Nested Graph Convolutional Network. *Journal of Systems and Software*, *204*, 111775. https://doi.org/10.1016/j.jss.2023.111775

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. http://dx.doi.org/10.2139/ssrn.3440802

Philip, A., & Saravanaguru, R. (2022). Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *Journal of King Saud University – Computer and Information Sciences*, *34*(7), 4031–4046. https://doi.org/10.1016/j.jksuci.2022.06.001

Papadouli, V., & Papakonstantinou, V. (2023). A preliminary study on artificial intelligence oracles and smart contracts: A legal approach to the interaction of two novel technological breakthroughs. *Computer Law & Security Review*, *51*, 105869. https://doi.org/10.1016/j.clsr.2023.105869

Perez, A. J., & Zeadally, S. (2023). Secure and privacy-preserving crowdsensing using smart contracts: Issues and solutions. *Computer Science Review*, *43*, 100450. https://doi.org/10.1016/j.cosrev.2021.100450

Pishdad-Bozorgi, P., & Han Yoon, J. (2022). Transformational approach to subcontractor selection using blockchain-enabled smart contract as trust-enhancing technology. *Automation in Construction*, *142*, 104538. https://doi.org/10.1016/j.autcon.2022.104538

Sathiyamurthy, K., & Kodavali, L. (2023). Bayesian network-based quality assessment of blockchain smart contracts. In *Advances in Computers*. Elsevier. https://doi.org/10.1016/bs.adcom.2023.07.004

Vatiero, M. (2023). Smart contracts vs incomplete contracts: A transaction cost economics viewpoint. *Computer Law & Security Review*, *46*, 105710. https://doi.org/10.1016/j.clsr.2022.105710

Wang, Y., Chen, X., Huang, Y., & Hao-Nan, Z. (2023a). An empirical study on real bug fixes from solidity smart contract projects. *Journal of Systems and Software*, *204*, 111787. https://doi.org/10.1016/j.jss.2023.111787

Wang, L., Cheng, H., Zheng, Z., Yang, A., & Xu, M. (2023b). Temporal transaction information-aware Ponzi scheme detection for ethereum smart contracts. *Engineering Applications of Artificial Intelligence*, *126*, Part C, 107022. https://doi.org/10.1016/j.engappai.2023.107022

Zhang, T., Feng, T., & Ming-li, C. (2023). Smart contract design and process optimization of carbon trading based on blockchain: The case of China's electric power sector. *Journal of Cleaner Production*, *397*, 136509. https://doi.org/10.1016/j.jclepro.2023.136509

Author information

Tharika Dishani Lamappulage Donn – MSc, Master Student, University of Greenwich
Address: Old Royal Naval College, Park Row, London SE10 9LS, United Kingdom
E-mail: tharikadishani@gmail.com
ORCID ID: https://orcid.org/0009-0004-6820-8788
Google Scholar ID: https://scholar.google.com/citations?user=zc0kRegAAAAJ

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – July 27, 2023
Date of approval – October 19, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:347.45/.47:339
EDN: https://elibrary.ru/gvbwbi
DOI: https://doi.org/10.21202/jdtl.2023.45

Смарт-контракты в международной торговле: европейские правовые стратегии преодоления трудностей

Тарика Дишани Ламаппулаге Донн

Гринвичский университет
г. Лондон, Великобритания

Ключевые слова

алгоритмический код,
компьютерная программа,
международная торговля,
право,
смарт-контракт,
технологии блокчейн,
цифровизация,
цифровое соглашение,
цифровые технологии,
электронная форма

Аннотация

Цель: присущая смарт-контрактам автоматизация делает их привлекательным инструментом для применения в сфере глобальной торговли, особенно с целью автоматизации транзакций. Прогнозируемая перспектива окажет серьезное влияние на международные экономические отношения и трансформацию правил международной торговли, что фокусирует настоящее исследование на выявлении возможностей трансформации указанных правил и принимаемых европейскими странами политико-правовых стратегий внедрения смарт-контрактов в международную торговлю.

Методы: исследование текущего состояния регулирования международной торговли в условиях процессов цифровизации, оцифровки контрактов и распространения смарт-контрактов основывается на совокупности формально-юридического и сравнительно-правового методов, позволяющих изучить правила международной торговли, проанализировать в сравнении политико-правовые позиции Великобритании и Европейского союза по вопросу внедрения смарт-контрактов в международную торговлю, а также спрогнозировать юридические последствия использования смарт-контрактов в указанной области (прогностический метод).

Результаты: исследование показывает, что распространение смарт-контрактов имеет существенные последствия для международной торговли и ее регулирования. Обладая многочисленными преимуществами,

такими как повышенная эффективность, снижение затрат и широкая доступность, они при согласовании традиционных правовых принципов с цифровой средой могут привести к юридическим проблемам, в частности, касающимся аутентификации субъектов, возможности принудительного исполнения от конкретных обстоятельств дела, вопросов юрисдикции.

Научная новизна: имеющаяся литература по вопросам трансформации регулирования международной торговли в условиях процессов цифровизации и распространения смарт-контрактов дополняется результатами сравнительного анализа правовых позиций, имеющихся на европейском правовом пространстве и выработанных на основе проблем, уроков и достижений при внедрении смарт-контрактов в международную торговлю.

Практическая значимость: понимание юридических последствий смарт-контрактов имеет важное значение для предприятий, участвующих в международной торговле. Исследование дает представление о правовых позициях Великобритании и Европейского союза, на основе которых можно выработать рекомендации компаниям, ориентирующимся в цифровом ландшафте. Директивные органы также могут извлечь пользу из полученных результатов для разработки соответствующих правовых актов, которые уравновешивают преимущества смарт-контрактов с необходимостью правовой определенности и защитой в международной торговле.

Для цитирования

Ламаппулаге Донн, Т. Д. (2023). Смарт-контракты в международной торговле: европейские правовые стратегии преодоления трудностей. *Journal of Digital Technologies and Law*, *1*(4), 1042–1057. https://doi.org/10.21202/jdtl.2023.45

Список литературы

Ante, L. (2021). Smart contracts on the blockchain – A bibliometric analysis and review. *Telematics and Informatics*, *57*, 101519. https://doi.org/10.1016/j.tele.2020.101519

Bandara, E., Ng, W. K., Ranasinghe, N., & De Zoysa, K. (2019). Aplos: Smart Contracts made smart. In J. F. Ashish, Gh. R. Oliveira, P. L. Zhou (Eds.), *Communications in Computer and Information Science* (pp. 431–445). https://doi.org/10.1007/978-981-15-2777-7_35

Blaszczyk, M. (2023). *Smart contracts, Lex cryptographia, and transnational contract theory*. SSRN. https://doi.org/10.2139/ssrn.4319654

Buigut, S., & Kapar, B. (2023). How did Brexit impact EU trade? Evidence from real data. *The World Economy*, *46*(6), 1566–1581. https://doi.org/10.1111/twec.13419

Casolari, F., Taddeo, M., Turillazzi, A., & Floridi, L. (2023). How to improve smart contracts in the European Union Data Act. *Digital Society*, *2*(1). https://doi.org/10.1007/s44206-023-00038-2

Chu, H., Zhang, P., Dong, H., Xiao, Y., Shunhui, J., & Wenrui, L. (2023). A survey on smart contract vulnerabilities: Data sources, detection and repair. *Information and Software Technology*, *159*(107221). https://doi.org/10.1016/j.infsof.2023.107221

Durovic, M., & Willett, C. (2023). A legal framework for using smart contracts in Consumer Contracts: Machines as servants, not masters. *The Modern Law Review*. https://doi.org/10.1111/1468-2230.12817

Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law & Security Review*, *35*(1), 69–88. https://doi.org/10.1016/j.clsr.2018.09.003

Fatima, S. (2023). Employability of a Research Method and Methodology in a Socio-Legal Study. *Global Social Sciences Review*, *VIII*(I), 341–351. https://doi.org/10.31703/gssr.2023(VIII-I).31

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution? *Telecommunications Policy*, *45*(2), 102081. https://doi.org/10.1016/j.telpol.2020.102081

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Corrias, G., Moncada, R., Cavallaro, A., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, *4*(3), 100142. https://doi.org/10.1016/j.bcra.2023.100142

Gunay, S., & Kaskaloglu, K. (2022). Does utilizing smart contracts induce a financial connectedness between Ethereum and non-fungible tokens? *Research in International Business and Finance*, *63*, 101773. https://doi.org/10.1016/j.ribaf.2022.101773

Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, *177*, 102857. https://doi.org/10.1016/j.jnca.2020.102857

Hoekstra, J. (2021). Political barriers in the ratification of international commercial law conventions. *Uniform Law Review*, *26*(1), 43–66. https://doi.org/10.1093/ulr/unab003

Hughes, E., Graham, L., Rowley, L., & Lowe, R. (2018, July 1). Unlocking blockchain: Embracing new technologies to drive efficiency and empower the citizen. *The Journal of The British Blockchain Association*, *1*(1), 63–72. https://doaj.org/article/6b966411b40746de873b99f25546bfca

Ji, B., Zhang, M., Xing, L., Li, X., Li, Ch., Han, C., & Wen, H. (2023). Research on optimal intelligent routing algorithm for IoV with machine learning and smart contract. *Digital Communications and Networks*, *9*(1), 47–55. https://doi.org/10.1016/j.dcan.2022.06.012

Kim, N. (2023). National ID for public purpose. *Georgetown Law Technology Review*, *7*(2). https://clck.ru/36kzR3

Kirli, D., Couraud, B., Robu, V., & Salgado-Bravo, M. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, *158*, 112013. https://doi.org/10.1016/j.rser.2021.112013

Liu, L., Wei-Tek, T., Zakirulm A., Hao, P., & Mingsheng, L. (2022). Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum. *Future Generation Computer Systems*, *128*, 158–166. https://doi.org/10.1016/j.future.2021.08.023

Liu, H., Fan, Y., Feng, L., & Wei, Z. (2023). Vulnerable smart contract function locating based on Multi-Relational Nested Graph Convolutional Network. *Journal of Systems and Software*, *204*, 111775. https://doi.org/10.1016/j.jss.2023.111775

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. http://dx.doi.org/10.2139/ssrn.3440802

Philip, A., & Saravanaguru, R. (2022). Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *Journal of King Saud University – Computer and Information Sciences*, *34*(7), 4031–4046. https://doi.org/10.1016/j.jksuci.2022.06.001

Papadouli, V., & Papakonstantinou, V. (2023). A preliminary study on artificial intelligence oracles and smart contracts: A legal approach to the interaction of two novel technological breakthroughs. *Computer Law & Security Review*, *51*, 105869. https://doi.org/10.1016/j.clsr.2023.105869

Perez, A. J., & Zeadally, S. (2023). Secure and privacy-preserving crowdsensing using smart contracts: Issues and solutions. *Computer Science Review*, *43*, 100450. https://doi.org/10.1016/j.cosrev.2021.100450

Pishdad-Bozorgi, P., & Han Yoon, J. (2022). Transformational approach to subcontractor selection using blockchain-enabled smart contract as trust-enhancing technology. *Automation in Construction*, *142*, 104538. https://doi.org/10.1016/j.autcon.2022.104538

Sathiyamurthy, K., & Kodavali, L. (2023). Bayesian network-based quality assessment of blockchain smart contracts. In *Advances in Computers*. Elsevier. https://doi.org/10.1016/bs.adcom.2023.07.004

Vatiero, M. (2023). Smart contracts vs incomplete contracts: A transaction cost economics viewpoint. *Computer Law & Security Review*, *46*, 105710. https://doi.org/10.1016/j.clsr.2022.105710

Wang, Y., Chen, X., Huang, Y., & Hao-Nan, Z. (2023a). An empirical study on real bug fixes from solidity smart contract projects. *Journal of Systems and Software*, *204*, 111787. https://doi.org/10.1016/j.jss.2023.111787

Wang, L., Cheng, H., Zheng, Z., Yang, A., & Xu, M. (2023b). Temporal transaction information-aware Ponzi scheme detection for ethereum smart contracts. *Engineering Applications of Artificial Intelligence*, *126*, Part C, 107022. https://doi.org/10.1016/j.engappai.2023.107022

Zhang, T., Feng, T., & Ming-li, C. (2023). Smart contract design and process optimization of carbon trading based on blockchain: The case of China's electric power sector. *Journal of Cleaner Production*, *397*, 136509. https://doi.org/10.1016/j.jclepro.2023.136509

Сведения об авторе

Ламаппулаге Донн Тарика Дишани – магистр права, магистр наук, Гринвичский университет
Адрес: Великобритания, г. Лондон, Парк Роу, SE10 9LS, Старый Королевский военно-морской колледж
E-mail: tharikadishani@gmail.com
ORCID ID: https://orcid.org/0009-0004-6820-8788
Google Scholar ID: https://scholar.google.com/citations?user=zc0kRegAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.89.27 / Обязательственное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 27 июля 2023 г.
Дата одобрения после рецензирования – 19 октября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.46

Remote Methods of Conducting Transactions Using Digital Technologies

Tatyana A. Savelyeva

Novosibirsk Law Institute (branch) of Tomsk State University
Novosibirsk, Russia

Keywords

artificial intelligence,
balance of interests,
blockchain,
digital technologies,
distant contract,
distant transaction,
electronic document,
information technologies,
law,
smart contract

Abstract

Objective: to substantiate the need to identify new contractual constructs (models) taking into account the specific relations associated with the use of remote method of contract conclusion through digital technologies and to study the possible risks for their participants.

Methods: along with special legal methods, the method of critical analysis was fundamental for the research process, which allowed us to evaluate and interpret the main sources and norms of civil law in relation to distant transactions. It also allowed assessing the current state of legislation in this area in the context of developing processes of digitalization and technologization of civil-law relations.

Results: a critical analysis of the current state of legal regulation of remote ways of concluding contracts is presented, their classification is given. It is concluded that the digital technologies development gives rise to new remote ways of transactions, as well as fills with new content the procedures of contract conclusion, traditional for civil law. The expediency of singling out the concept of a "distant transaction" as a legal category in order to create a special civil-law regime is substantiated, and the basic concept being that of a "distant contract". Certain types of distant contracts are analyzed to substantiate the need for special legal regimes in cases when the distant method of contract conclusion is combined with the use of digital technologies. It poses such problems as the distribution of risks of technological failures, hacker attacks, compliance with the balance of interests of the parties taking into account information asymmetry, and the need to protect the weaker party.

Scientific novelty: an attempt is made to define such concepts as a "distant contract" and a "distant transaction" and to identify their features. The expediency is substantiated of considering a distant contract as a separate legal construction (model) of the contract. Within this framework, a special legal regime should be developed and fixed, which can be extended to unilateral distant transactions. The problems of legal regulation caused by the use of information technologies are formulated, and legal constructions for their solution are proposed.

Practical significance: the final conclusions and proposals can be used both in contractual practice by the participants of civil turnover and for the normative consolidation of the concept and features of "distant contract", "distant transaction". A special legal regime can be created, taking into account the specificity generated by the use of digital technologies.

For citation

Savelyeva, T. A. (2023). Remote Methods of Conducting Transactions Using Digital Technologies. *Journal of Digital Technologies and Law, 1*(4), 1058–1086. https://doi.org/10.21202/jdtl.2023.46

Contents

Introduction

The development of digital technologies affects all spheres of human activity, including the relationship of participants in civil turnover when signing and executing transactions.

Digital technologies allow participants in civil turnover to negotiate, enter into contractual relations, exchange documents, execute and accept execution, and communicate their will to the other party remotely. At the same time, the use of digital technologies makes remote interaction between parties to a contract fundamentally different from the "pre-digital" era.

Current legislation tries to take the development of information technologies into account. For example, the Civil Code of the Russian Federation (hereinafter – CC RF, or the Code)[1] was supplemented in 2019 with norms providing for the possibility of concluding a contract in electronic form (by exchanging electronic messages, by concluding a single electronic document)[2].

Meanwhile, the legislator does not single out remote transactions as a separate category. A legitimate question arises as to the expediency of such separation given the practical needs of civil turnover, as well as from the doctrinal viewpoint. Is it sufficient that the law provides for an electronic form of transaction?

The criterion of the correctness answer to this question should be the test regarding the balance of interests of the parties to remotely concluded transactions. Is it achieved within the current legal regulation, given that there is no special legal regime due to the remote nature of interaction between the parties, which excludes direct perception of the other party's will, familiarization with the subject of the transaction at the time of its execution, etc.?

It should be noted that a lot of legal literature is devoted to the study of the electronic form of the transaction. However, a number of important aspects of the parties' remote interaction, going beyond the form of the transaction, remain without due attention, including the issue of observing the balance of interests of the parties.

Meanwhile, it is obvious that the effectiveness of digitalization of remote ways of transactions should be estimated through the prism of observing the balance of interests of the parties. Otherwise, neither the objectives of digitalization nor the objectives of legal regulation will be achieved.

It should be noted that the conclusion of a contract by exchanging messages, letters, as well as by signing a single document, are traditional for civil law and are regulated in sufficient detail in the CC RF.

---

1 Civil Code of the Russian Federation (Part 1) of 30.11.1994 No. 51-FZ (with amendments). SPS KonsultantPlyus. https://clck.ru/36brfs

2 On making amendments in Part 1, 2, and Article 1124 of Part 3 of the Civil Code of the Russian Federation. No. 34-FZ of 18.03.2019. (2019). Collection of legislation of the Russian Federation, 12,Art. 12.

The possibility of exchanging electronic messages using digital technologies does not, at first glance, change the essence of the traditional approach, as only the form of the message changes. The same can be said about the possibility of concluding a contract by signing a single electronic document.

However, such a view is superficial. Indeed, the use of digital technologies inevitably generates risks of technological nature, including risks of destruction or distortion of the electronic document content, risks of violating the interests of a party due to a probable information asymmetry, etc.

This study is devoted to the analysis of remote ways of making transactions using digital technologies. The objective is to assess how traditional approaches to the civil law contract conclusion and the current civil law legislation meet the new challenges arising due to the active use of digital technologies in the interaction between the contractual relations participants.

The paper consists of three sections. In the first section, we analyze remote ways of concluding a contract and making unilateral transactions, as well as their peculiarities related to the use of digital technologies. The objective is to decide whether or not it is appropriate to single out "remote contract" and "remote transaction" as legal concepts. The second section of the work is devoted to reviewing certain types of distant contracts in the aspect of the balance of the parties' interests. The third section studies the aspects of the parties' remote interactions, which are beyond the scope of private law regulation, but may serve to confirm or refute the expediency of considering remote transactions as a legal concept and establishing a special legal regime.

1. Notion and types of distant transactions

1.1. Scope of use and regulation of the remote method of contract conclusion

The remote method of concluding various transactions has become widespread in civil turnover. Remote trade, remote banking, including settlements with the use of bank cards, crediting and even conclusion of real estate transactions in a remote format have become ingrained in our everyday lives.

Any transaction where the parties use remote communication means, including postal messages, e-mail, SMS messages, Internet, etc., instead of physical presence at the stage of negotiations and transaction conclusion, can be referred to the remote mode of transactions.

As for the legal regulation of the remote method of transactions conclusion, it should be noted that there is no systematic approach taking into account the specificity of relations associated with the use of this method of contract conclusion in various spheres. For example, the remote method of retail sale of goods is quite thoroughly regulated by the legislation[3].

[3] Civil Code of the Russian Federation (Part 2) 14-FZ of 26.01.1996 (ed. of 24.07.2023) (with amendments valid since 12.09.2023), Art. 497. SPS KonsultantPlyus. https://clck.ru/36briF ; On protection of consumer rights. No. 2300-1 of 07.02.1992 (with amendments), Art. 26.1. SPS KonsultantPlyus. https://clck.ru/36brjV ; Decree of the Government of the Russian Federation No. 2463 of 31.12.2020. (2020). SPS KonsultantPlyus. https://clck.ru/36brka

Speaking about other spheres of using the remote method of contract conclusion, it should be noted that there is no special legal regulation, with rare exceptions, which will be considered further. This approach is due to the fact that the legislator probably sees no need for such regulation.

In view of the above, it seems important to analyze the existing general legal norms relating to the remote method of concluding contracts in order to assess the sufficiency of legal regulation under the rapid development of digital technologies and their practical implementation.

The process of digitalization requires a rethinking of many traditional views on the contractual sphere, including the remote mode of contracting.

In our analysis, we leave out the issues of using artificial intelligence in the field of interaction between parties to civil law contracts.

At the same time, one cannot but recognize the increasing influence of artificial intelligence on all spheres of our life. One of such manifestations is the transfer of communications to the virtual environment (cyberspace) (Filipova, 2023). In view of the above, the influence of artificial intelligence on the interaction between the parties in the remote way of concluding transactions deserves a separate study.

By virtue of clause 1 of Art. 160 of the CC RF, a transaction in writing must be made by drawing up a document expressing its content and signed by the person(s) making the transaction or by duly authorized persons. The written form of a transaction shall be deemed to be complied with also in case a person makes a transaction with the help of electronic or other technical means which allow reproducing the transaction content on a material medium in an unaltered form. The requirement for a signature shall be deemed to be fulfilled if any method is used that allows reliably determining the person who has expressed the will. The law, other legal acts and the agreement of the parties may provide for a special way of reliably determining the person who expressed the will.

Any contract concluded between absentees may be qualified as a distant transaction in the broad sense.

The Code regulates in detail the procedure for concluding a contract between absentees, which includes sending a proposal (offer), its consideration by the acceptor, sending an acceptance, and its receipt by the offerer. By virtue of clause 1 of Art. 433 of the CC RF, "the contract is recognized as concluded at the moment when the person who had sent the offer receives its acceptance"[4].

The legislator has established the consequences of sending an offer containing a term for acceptance (Art. 440 of the CC RF), an offer that does not contain a term for acceptance (Art. 441 of the CC RF), the consequences of late acceptance (Art. 443 of the CC RF) and so on.

The remote method of concluding a contract can also include the conclusion of a contract through the acceptor's conclusive actions. For example, by virtue of clause

[4] Civil Code of the Russian Federation (Part 1) of 30.11.1994 No. 51-FZ (ed. of 24.07.2023) (with amendments valid since 01.10.2023). SPS KonsultantPlyus. https://clck.ru/36eEQ9

3 of Art. 438 of the CC RF, the performance by the person who received the offer, within the period established for its acceptance, of actions to fulfill the terms of the contract specified in it (shipment of goods, provision of services, performance of work, payment of the appropriate amount, etc.) is considered an acceptance, unless otherwise provided by law, other legal acts, or specified in the offer.

Digitalization, namely, the possibility of sending an offer and acceptance using information technologies, makes it necessary to take a new look at the procedure of concluding a contract between absentees and to single out in a separate category contracts concluded remotely by exchanging documents not in the traditional paper form.

Moreover, the scope of the remote method of concluding a contract covers not only exchanging offer-acceptance letters or messages, but also signing a single document in electronic form.

In 2019, important amendments were made to the CC RF, in particular to Article 434 of the Code. By virtue of clause 2 of this article, a contract in writing may be concluded by drawing up a single document (including an electronic one) signed by the parties, or by exchanging letters, telegrams, electronic documents or other data in accordance with the rules of the second paragraph of clause 1 of Art. 160 of the Code.

As is known, agreements on real estate (Articles 550, 560, 651, 658 of the CC RF), a corporate agreement (Article 67.2 of the CC RF), an agreement on establishment of a joint stock company (Article 98 of the CC RF), etc. are subject to conclusion by signing a single document.

Contracts concluded by signing a single electronic document can certainly be referred to distant contracts.

A number of contracts concluded by means of a single document require notarization. In particular, notarial certification is required for a rent contract (Article 584 of the CC RF), as well as a transaction aimed at alienation of a share in the authorized capital of a limited liability company (clause 11 of Article 21 of the Law on Limited Liability Companies)[5].

Participants of civil turnover may notarize transactions in cases provided for by the agreement of the parties, even if this form is not required by law for transactions of this type (clause 2 of Article 163 of the CC RF).

As part of the digitalization process in our country, in 2019 the notary officials were empowered to perform notary acts remotely. One of the novelties was the rules of certifying a transaction by two or more notaries without their personal presence[6].

This refers to the situation when the parties to the transaction are located in different regions and make the transaction without leaving their location. In this case, notarization of the transaction is carried out by notaries of different regions. The parties to the transaction

[5] On limited liability companies. No. 14-FZ of 08.02.1998 (ed. of 13.06.2023). SPS KonsultantPlyus. https://clck.ru/36brni

[6] On amendments to the Fundamentals of legislation of the Russian Federation on notary and to certain legislative acts of the Russian Federation. No. 480-FZ of 27.12.2019. (2019). Collection of legislation of the Russian Federation, 52 (Part I), Art. 7798.

prepare a draft agreement with the help of notaries, and then sign the text on paper and in electronic form. Such contracts may also be referred to remote transactions.

An important category of distant transactions are smart contracts. Smart contracts can be used in various spheres and at different stages of contractual relations. Smart contracts allow consumers to choose a supplier and enter into a contractual relationship with them. When deployed on a blockchain, smart contracts can automatically enter into and enforce agreements (Kirli et al., 2022).

Notably, there is no legal definition of a smart contract. Different points of view regarding their legal nature have been expressed in the literature. The legal community is trying to find answers to the question whether it is possible to apply traditional contractual constructs to a smart contract and to what extent (Savelyev, 2016; Belov, 2021; Efimova, 2019; Churilov, 2020; Shelepina, 2021; Tsepov, & Ivanov, 2022; Chelysheva, 2022, Hsain et al., 2021).

Meanwhile, despite the controversy regarding the concept of smart contract, as was rightly noted in the literature, smart contracts are actually used in everyday life, e.g., when calling for a taxi, renting a car, etc. (Utkin, 2022).

According to some authors, "a smart contract is a computer program (or computer code) that can only be concluded using blockchain technology and allows automatically concluding, executing and terminating various contracts upon the occurrence of predetermined legal facts" (Efimova & Sizemova, 2019).

The draft Federal Law "On digital financial assets" gives the following definition: "A smart contract is an agreement in electronic form, the fulfillment of rights and obligations under which is carried out through the automatic execution of digital transactions in a distributed ledger of digital transactions in a sequence strictly defined by such an agreement and upon the occurrence of circumstances defined by it"[7].

This definition was excluded from the text of the law and while discussing the bill, the Committee on Economic Policy, Industry, Innovative Development and Entrepreneurship expressed a negative opinion on this issue. The Committee pointed out that "a smart contract is essentially a computer algorithm that allows participants of the distributed ledge to exchange assets; it is a technology and cannot be recognized as a type of civil law contract". The Committee's Conclusion stated that the only and sufficient rule for "smart contracts" is stipulated by Article 309 of the CC RF: "the fact of a transaction execution by a computer program is not disputed (except for cases of interference with the program). After the users are identified in the system, their behavior is subject to the algorithm of the computer program organizing the network, and the person "buying" a virtual item (digital right) will receive this item automatically"[8].

---

7 On digital financial assets: draft Federal Law No. 419059-7 (edition submitted to the Russian State Duma, text as of 20.03.2018). SPS KonsultantPlyus. https://clck.ru/36bron

8 Conclusion of the Committee on economic policy, industry, innovative development and entrepreneurship of 03.04.2018 No. 3.8/522 "On the draft Federal Law No. 419059-7 "On digital financial assets". SPS KonsultantPlyus. https://clck.ru/36brpn

Researchers rightly point out that one of the most pressing problems of smart contracts is that they are based on procedural programming languages. A code in a procedural language usually must specify how to solve a problem by explicitly providing clear instructions that govern its behavior (Ferro et al., 2023).

The issues related to smart contracts require a separate study due to the voluminous nature of the material, the ambiguity of some starting positions both in understanding smart contracts and in understanding the reliability of the results obtained when using smart contracts, especially given that they are subject to attacks (Aquilina et al., 2021).

In this paper, smart contracts will be touched upon only to the extent necessary for analyzing distant transactions as a legal category in general.

Speaking of the legal regulation of remote transactions, it should be noted that their separate relevant aspect is how to ensure the confidentiality of information, including personal information.

This issue becomes especially relevant in transactions with a foreign element, when there is an export of personal information. It is no coincidence that on February 24, 2023, the Cyberspace Administration of China (CAC) issued "Measures on standard contracts for exporting personal information" (Kennedy, 2023).

We believe that the issues of personal data export within remote transactions with a foreign element require a separate study in order to legislatively stipulate mechanisms to control the transfer of such data outside Russia.

Continuing the theme of legal regulation of digital technologies used in remote interaction between the transaction parties, it is necessary to point out another aspect that goes not only beyond the scope of civil law regulation, but also, perhaps, beyond the scope of legal regulation in general. It is about the differences in the legal consciousness of lawyers who are engaged in lawmaking and law enforcement activities, and subjects who carry out technical development of the use of digital environment in various spheres of human life, including remote interaction. An interesting study in this area has been conducted by foreign authors, who have identified fundamentally different views on security in lawyers and robotics specialists (Rompaey et al., 2022).

This issue is beyond the scope of our paper. However, we cannot but note this problem as one of the possible reasons for the difficulties of introducing technical achievements in jurisprudence.

Summarizing the above, we can state that the remote way of concluding a contract, i. e. without simultaneous personal presence of the parties and expression of will in the place of conclusion of the contract, is not new for the legislation. Legal regulation of the procedure for concluding a contract between absentees has always been rather detailed. At the same time, the development of digital technologies gives rise to new remote ways of concluding contracts and fills the previously established procedures of interaction between the parties with new content.

1.2. On the notion of distant transaction. Types of distant contracts and other transactions

The current legislation does not consider remote transactions as a separate category, nor establish a special legal regime for their participants, only regulating the electronic form of a transaction.

As it was stated above, the remote method of contract conclusion is not new for our legislation. The exchange of written messages is a classic way of concluding a contract.

At the same time, one should admit that the remote method of interaction between the parties to the transaction gives rise to certain specificity in the relationship. Actually, this method excludes a party's direct familiarization with its subject matter at the stage of will expression and limits the possibility of the party identification, as well as direct perception of the will of the other party.

Together with this specificity, the use of digital technologies significantly affects interaction between the parties, inevitably generating risks caused by the use of these technologies.

This allows questioning the expediency of considering a distant transaction as a legal category, as well as the need to create a special legal regime, taking into account the balance of interests of the transaction parties. After all, remote interaction using digital technologies gives rise to issues related to information asymmetry, the need to recognize a transaction participant as a weak party and provide them with adequate means of protection, distribute technological risks, etc.

Earlier, we have considered the issues related to the legal regulation of remote methods of civil law contracts conclusion, among which we can distinguish:

1) contracts concluded with a distant method of retail selling of goods;

2) contracts concluded by means of exchange of written messages in the classical form;

3) contracts concluded through the exchange of electronic messages;

4) contracts concluded by means of conclusory actions;

5) contracts concluded remotely by signing a single document in an electronic form;

6) contracts concluded remotely in a notary form (by certification by two or more notaries);

7) smart contracts.

A question arises whether all these contracts can be considered remote. To answer this question, it is necessary to define the concept of a distant contract.

If a distant contract is understood as any contract that is concluded without the parties' personal presence at the moment of will expression at the place of the contract conclusion, then almost all of the above contracts can be considered distant contracts.

We believe that such an understanding of a distant contract would be unnecessarily broad, as it would not meet the objectives of creating a special legal regime for this type of contract.

In our opinion, a special legal regime is required where the remote method of concluding a contract is combined with the use of digital technologies. It is the use of digital technologies that poses such problems as distributing the risks of technological failures, hacker attacks, observing the balance of interests of the parties, protecting the weaker party, which should be solved within the framework of a special legal regime.

If we reduce the remote interaction between the parties during the contract conclusion and execution only to the specifics of the contract form (the fact that the contract is concluded in electronic form), then all the above aspects will remain beyond the scope of attention.

At the same time, one cannot deny the importance of the issues related to the contract conclusion in electronic form. Here, it is very important to master certain skills to work with Internet services, to increase the legal literacy of civil circulation participants; lawyers must study more deeply the peculiarities of the electronic form of contract and understand their peculiarities compared to a classical contract (Tărchilă & Nagy, 2015).

The expediency of considering a distant contract as an independent legal category is that it allows shifting the focus from the contract form to the specifics of establishing the contract content, the scope of rights and obligations arising, the distribution of risks stemming from the remote nature of interaction between the parties.

From these positions, the following types of distant contracts should be considered:

1) contracts concluded on the Internet;

2) contracts concluded through the exchange of electronic messages;

3) contracts concluded remotely by signing a single document in an electronic form;

4) contracts concluded remotely in a notary form (by certification by two or more notaries);

5) smart contracts.

All the above types of contracts are similar in that the parties interact remotely at the pre-contractual stage, at the stage of contract conclusion and, as a rule, at the stage of contract execution. The expression of will is mediated, and the will is perceived by the other party through information technologies.

In this case, one of the parties to the contract may be the right holder of the information resource through which the will is expressed. Moreover, this party forms the rules of remote interaction, thus having an informational advantage in the contractual process.

All this requires that the other party be provided with certain guarantees, which are possible within the framework of a special legal regime. Within the framework of this legal regime, at least the following issues should be resolved:

– the criteria for establishing the status of the contract parties, recognizing one of them as a weak party;

– the conditions of liability of the parties, including the application of the “strict” liability principle (regardless of fault), and the limits of its application;

– the party bearing the risks of technological failures and hacker attacks;

– the distribution of the burden of proof between the parties.

We believe the legislator should consider a distant contract to be a separate contractual structure, along with other contractual structures stipulated in Part 1 of the CC RF (option contract, subscription contract, etc.). As a justification, it can be pointed out that such a contract has no less specificity, and the emerging relations require the establishment of a special legal regime.

In the subsequent part of this paper we will consider the issues of observing the parties' balance of interests in relation to certain types of distant agreements listed above. This will serve as an additional argument in support of the expediency of singling out a distant agreement as a separate contractual construction.

The next issue that should be touched upon is unilateral transactions, namely, whether the concept of a remote unilateral transaction may exist along with the concept of a distant contract.

When answering this question, it is necessary to proceed from the essence of a unilateral transaction and the consequences of its conclusion.

By virtue of clause 2 of Article 154 of the CC RF, a unilateral transaction is a transaction, for the execution of which the expression of the will of one party is necessary and sufficient, in accordance with the law, other legal acts or the agreement of the parties.

Taking into account the content of Article 160 of the CC RF, a unilateral transaction can be made in an electronic form.

By virtue of Article 155 of the CC RF, a unilateral transaction creates obligations for the person who made the transaction. It may create obligations for other persons only in cases established by law or by agreement with these persons.

It is the unilateral nature of will expression, the absence of consequences in the form of creating obligations for other persons that raises doubts about the possibility of remote unilateral transactions.

At the same time, it should be noted that unilateral transactions in a number of cases can be recognized as remote ones.

For example, the literature shows the prospects of remote participation of a notary in the certification of wills (Yatsenko, 2019; Mikhailova, 2020). In this case, a will is a remote transaction.

One more important aspect should be taken into account. Among unilateral transactions, transactions requiring perception and transactions not requiring perception are distinguished (Akuzhinov, 2020). Regarding transactions requiring perception, A. V. Egorov points out: "The essence of distinguishing this category is that this type of unilateral transactions becomes effective not from the moment of the will expression, but from the moment the will expression is received by the addressee" (Egorov, 2015).

One should note that most unilateral transactions are transactions requiring perception. They include, in particular, unilateral refusal from the contract (fulfillment of the contract). By virtue of Article 450.1 of the CC RF, the right to unilateral refusal from the contract (fulfillment of the contract) may be exercised by the authorized party by notifying the other party of the refusal from the contract (fulfillment of the contract). The contract is terminated

from the moment of receipt of this notice, unless otherwise provided by this Code, other laws, other legal acts, or the contract.

There are no obstacles for declaring a unilateral withdrawal from the contract in an electronic form (of course, if there are grounds for withdrawal from the contract out of court).

In this case we have, at first glance, a contradictory situation. On the one hand, the right to withdraw from the contract does not depend on the counterparty, their behavior and attitude to this being irrelevant in terms of legal consequences for the person refusing the contract. From this viewpoint, unilateral repudiation of the contract must not be considered as a remote transaction.

On the other hand, the contract repudiation must not only be stated but also perceived by the counterparty. This means that, although the behavior of the counterparty is irrelevant to the person repudiating the contract, nevertheless the performance of a unilateral transaction involves interaction with the counterparty.

If such interaction is carried out using information technologies, there is every reason for establishing a special legal regime discussed earlier. The above indicates that unilateral transactions requiring perception may be referred to remote transactions, if the communication of will to the counterparty is carried out using digital technologies.

This said, we believe that the basic concept should be the concept of a distant contract. A special legal regime should be developed and enshrined within the structure of a distant contract, which can be extended to unilateral transactions.

2. Providing the balance of interests of the parties in certain distant transactions

2.1. Contracts concluded via Internet sites

Transacting on the Internet has become so widespread that it makes it necessary to consider the way in which transactions are conducted from the viewpoint of balancing the parties' interests.

First of all, it should be noted that when the conclusion of certain agreements is available exclusively through participation in Internet services, this means that it is impossible to carry out various forms of activity without Internet access (Lim & Pan, 2021). This should be considered as a factor that violates the rights of potential consumers.

This aspect goes beyond the scope of private law regulation and deserves a separate study. However, it cannot be ignored when it comes to balancing the interests of civil turnover participants. Below we will consider the peculiarities of the order of concluding contracts via Internet sites in the aspect of civil law regulation. Any contract is an agreement of the parties, the content of which is a set of conditions that the parties have agreed upon.

Therefore, it is important to familiarize the user with the contract terms (the offer published on the website). After all, mindlessly clicking "I agree" button threatens with unpredictable consequences.

The main options for expressing the user's consent to the agreement terms published on the website depend on the way the agreement terms are published:

1. The text of the agreement is placed directly on the website page.

2. The offer is not placed directly on the site page; familiarization is possible by clicking on a hyperlink.

3. The site has a record of the user's implied consent to the terms and conditions in the case of continuing the use of the site.

In the latter case, doubts arise as to whether the contract can be considered concluded, which should be resolved taking into account the specific circumstances (Grin, 2019).

The order of concluding a contract via Internet sites violates the balance of interests of the parties. Due to the information inequality, a user is a weak party and should be endowed with appropriate means of protection, including the right, provided for in clause 2 of Article 428 of the CC RF, to demand amendment or termination of the contract with retrospective effect.

Summarizing the brief consideration of the contracts conclusion via Internet sites, we should state that such contracts meet the conditions sufficient to qualify them as adhesion contracts by virtue of Article 428 of the CC RF.

A way to maintain the parties' balance of interests would be to enshrine the rule on extending the adhesion contract regime to transactions made via Internet sites. At that, the website owner could be given the opportunity to exclude the effect of Article 428 of the CC RF if the website provides a technical opportunity for the consumer to participate in the development and adjustment of the agreement terms published on the website.

At the same time, one may agree that "the protection mechanisms provided for in clause 3 of Article 428 of the CC RF cannot be fully realized. It is a question of the absence of certain criteria in the legislation, allowing in practice to 'decipher' (or specify) whether legal relations imply inequality of bargaining power and determination of the contract terms by one of the parties only, which give the weaker party the mentioned legal guarantees" (Ovchinnikova, 2022).

We should agree that "the current regulation does not allow properly assessing the good faith and equality of the parties to the agreement, if the terms are formed by only one party using computer technology" (Kuzmina, & Lomakina, 2022).

Thus, the above allows concluding that the procedure for concluding contracts via Internet sites violates the parties' balance of interests. A user is a weak party due to information asymmetry and inequality of negotiation opportunities. This requires establishing a special legal regime to regulate the parties' relations within the procedure for such transactions.

In addition, a separate study is required to determine the expediency of legislative restriction of cases when the lack of availability of Internet services excludes the possibility of concluding contracts and entails limitation of access to goods, services or is an obstacle to the implementation of certain activities.

2.2. Contracts concluded by drawing up a single electronic document signed by the parties

Clause 2 of Article 434 of the CC RF provides that a contract in writing may be concluded by drawing up a single document (including electronic) signed by the parties.

Contracts are signed by electronic signatures[9]. Such a contract can be fully referred to a distant contract.

Some researchers express doubt that the possibility of using an electronic contract in the form of a single document appeared only after the amendments to the Code were made in 2019 (Kostikova, 2022).

This method of contract conclusion has become quite common in the real estate sphere. Contracts of sale and purchase, equity participation in the real estate objects construction, acts of acceptance and transfer of real estate are concluded in this form.

A detailed analysis of real estate transactions is beyond the scope of this study. However, the author would like to express her attitude to the remote execution of documents on the real estate transfer.

We believe the legislator's admission of such execution of deeds with real estate was hasty and insufficiently elaborated. In this case "risks arise for both parties. A buyer may face the fact that the real estate condition does not correspond to the way it was shown by a seller remotely via a video link. The process of proof will be complicated for the buyer because the videos are not recorded. Besides, the buyer, having signed the acceptance certificate, does not actually receive possession of the real estate.

For the seller, such registration of the transaction and the acceptance certificate may also create problems. For example, an unscrupulous buyer may claim that the deal was concluded under the influence of deceit or delusion, because the real estate was not inspected. The buyer can also claim that there was no actual transfer of real estate, the signing of the act was fictitious" (Savelieva, 2022).

The above indicates the presence of unresolved issues in connection with the remote interaction between the parties.

2.3. Contracts concluded remotely in notarized form (certified by two or more notaries)

The necessity and efficiency of using digital technologies in notary activity is beyond doubt. The remote notarization of transactions significantly simplifies the receipt of notary services by civil turnover participants.

Parties to a transaction located in different regions can conclude a contract and notarize it without leaving their location.

---

[9] On electronic signature. No. 63-FZ of 06.04.2011 (with amendments). SPS KonsultantPlyus. https://clck.ru/36brtE

The procedure for entering into such remote transactions includes the following main stages:

1) the parties preliminary agree on the contract terms and conditions;

2) each party selects a notary at the place of its location;

3) the notary executes a transaction passport in the software, including information on the transaction, participants, and representatives;

4) documents are added to a database;

5) the following information is recorded:

– a party signs information on the transaction participant with a simple electronic signature;

– a notary signs information on the transaction participant with a reinforced qualified signature;

6) notaries exchange information in the database and approve the transaction passport; the consequence is blocking of all operations with the agreed part of the transaction passport;

7) all notaries signs the transaction passport;

8) the transaction is certified, including:

– communication in videoconference format takes place, the parties (representatives) read the contract;

– each party signs a hard copy of the contract;

– each party signs the agreement with a simple electronic signature;

– notaries sign the agreement with a qualified electronic signature;

– the videoconference is completed and the notaries register the recording;

9) the documents are sent for state registration.

As we can see, the contract is executed and signed not only in electronic form, but also on paper. In this regard, the literature rightly raises the question of establishing the moment of expressing a person's will to make a transaction (Laptev & Solovyanenko, 2022).

In the aspect under consideration, in relation to this type of distant contracts, it is necessary to analyze to what extent the mechanism of such a transaction conclusion is a reliable guarantee for its participants.

It should be noted that the remote nature of the transaction certification does not reduce the level of requirements to the notary's activity of ensuring the transaction legality. As in the case of transaction certification in person, the notary verifies the legal status and capacity, establishes the will and the voluntariness of will expression, explains the consequences of the transaction, and verifies the legality of the transaction content.

At the same time, the use of information technologies, while creating convenience and comfort for transaction parties, has the downside of creating security risks in transactions. Such risks include the destruction or distortion of the electronic transactions content due to hacker attacks, introduction of a virus into the software. There may be problems with identification in remote interaction.

One should agree with E. A. Kirillova that "digitalization of the Russian notary provides new opportunities for citizens, but digital technologies are only an auxiliary tool, which

cannot replace a specialist like a notary who guarantees the legality of transactions" (Kirillova, 2021).

Also, questions arise about the consequences of technological failures, including the procedure for establishing the valid will of the parties, the procedure for claiming and evaluating digital evidence. Many of such questions, regrettably, remain unanswered so far.

2.4. Contracts concluded by exchange of electronic documents

When analyzing remote transactions in terms of balancing the parties' interests, one cannot but ignore contracts concluded by the exchange of electronic documents.

Analysis of judicial practice shows a significant number of disputes in which a court has to evaluate messages sent by e-mail ,[10], SMS, messengers,[11] etc.

It should be noted that similar issues are considered by foreign courts. As is known from literature, the general trend is to recognize such correspondence as admissible evidence, but this is not an unconditional provision. In each case a judge assesses the admissibility of such evidence (Kozlova & Sergacheva, 2022).

It seems that the legislator and/or, possibly, higher courts should give relatively clear guidelines to civil turnover participants regarding the possibility or impossibility of using remote communication without electronic signature in typical situations.

The safest way for civil turnover participants is to build a two-stage system when using electronic communication:

– concluding an agreement on the implementation of electronic document flow in the traditional form (indicating the specific types of documents and addresses for correspondence);

– actually exchanging electronic documents.

It should be noted that the conclusion of such agreements on electronic document flow is widespread in banking practice.

In other spheres, regrettably, such electronic document flow is practically never applied. The parties exchange scanned copies of draft contracts, protocols of disagreements, e-mail letters of offer, letters of acceptance, acts, or other documents to fulfill contractual obligations. At the same time, the parties execute no documents that legitimize electronic document flow.

[10] Enactment of the Presidium of the Supreme Appellation Court of the Russian Federation No. 18002/2012 of 12.11.2013 in case A47-7950/2011. SPS KonsultantPlyus. https://clck.ru/36brts

[11] Ruling of the Perm Cassation Court of general jurisdiction No. 88-22889/2020 of 30.10.2020 in case No. 2-1314/2019; Ruling of the Third Cassation Court of general jurisdiction No. 88-17185/2020 of 29.10.2020. SPS KonsultantPlyus. https://clck.ru/36brSB

Judicial practice is not uniform in the approaches to assessing correspondence not certified by electronic signature. Courts, as a rule, adjudicate disputes taking into account the previous practice of the parties, their behavior on obligations fulfillment after the correspondence, and provide assessments based on the performance of conclusive actions, subsequent approval, etc.

Participants of civil turnover should treat correspondence carefully, and in the most important cases conclude contracts/agreements concerning the procedure of remote interaction by means of electronic document flow.

To ensure predictability in the court disputes resolution, it is advisable to adopt clarifications at the level of the Supreme Court of the Russian Federation. Such clarifications should be based on the approach distinguishing between the stages at which correspondence was conducted and the establishment of various presumptions for proving the legitimacy of such correspondence.

Stricter criteria for the pre-contractual stage should be established. Correspondence without an electronic signature should not be regarded as legally significant (offer or acceptance). The exception, of course, should be cases when the parties concluded an agreement on electronic document flow.

This approach is justified by the fact that the sender has not yet entered into a relationship with the counterparty, has not confirmed their identity with an e-mail address and should not bear the risk that an unauthorized message will be sent via their mail.

In the case of subsequent stages, a presumption could be introduced that a message sent from the e-mail address specified in the contract is recognized as an expression of the will of the party to the contract.

The above indicates the need to develop clear guidelines to distribute the burden of proof when resolving disputes concerning the assessment of a contract “conclusion” in the course of remote interaction via electronic document flow.

3. Certain aspects of distant transactions beyond the scope of private law regulation

The need to single out distant transactions into a separate category is due, among other things, to a number of specific aspects outside the civil law regulation. Some of these aspects will be discussed in this section without claiming to be complete.

3.1. Assignment of public functions to private subjects (carriers of information on distant transactions)

The process of digitalization of the contractual sphere inevitably raises before the Russian legislator the problem of assigning public functions to private entities –carriers or keepers of information on the interaction of parties to contractual relations in the digital environment.

The assignment of public duties to private entities is not a new phenomenon. This can be confirmed by several examples from the banking sector, like the implementation of control functions by banks to combat criminal money legalization (laundering)[12] or performance of currency control functions[13].

Public functions are economically burdensome for credit organizations, as they require additional expenditures not directly related to making money. This contradicts with their civil-legal status as commercial organizations, the objective of which is to make profit. Meanwhile, the legislator has assigned these functions to credit organizations, and, obviously, the obligations to perform them should be considered as an integral part of their legal status.

Apparently, the issue will have to be solved in a similar way in relation to private entities – right holders and keepers of information on transactions in the information environment.

Foreign literature notes the transformation of the tasks faced by Internet providers. "Private actors do not only take part in designing rules for their sector but they are the ones responsible for defining infringements. Private actors do not simply assist public enforcement by implementing rules; today private actors proactively counter infringements and design strategies and tools to do so" (Tosza, 2021).

With the rapid development of remote transactions, it will be necessary to legislatively address the issue of assigning functions to Internet providers that go beyond their private interest. Such functions should include the obligation to store and provide information on transactions executed on the Internet (in the event of a dispute between the parties), as well as the obligation to monitor certain transactions or operations in order to protect the public interest.

3.2. Peculiarities of proof in disputes arising out of distant transactions

The remote nature of interaction between the parties to a transaction using digital technologies at the pre-contractual stage, at the stages of conclusion and execution of the contract gives rise to the question of the specifics of dispute resolution and the proving process in such disputes.

The current legislation does not establish any procedural peculiarities of dispute consideration, including collection and evaluation of digital evidence or distribution of the burden of proof.

[12] On combating criminal money legalization (laundering) and terrorism funding. No. 115-FZ of 07.08.2001 (with amendments). SPS KonsultantPlyus. https://clck.ru/36brw7

[13] On currency regulation and currency control. No. 173-FZ (with amendments) of 10.12.2003. SPS KonsultantPlyus. https://clck.ru/36brwh

In foreign literature we found a rather detailed study on the collection, storage, access to digital evidence related to the investigation of traffic accidents. The paper attempts to comprehensively investigate a range of issues related to proving transportation accidents, including methods of obtaining and transferring evidence in the digital environment, data access, role and responsibilities of various stakeholders (Philip & Saravanaguru, 2022).

The described structure of building an accident investigation using digital evidence is of interest not to forensics only.

As for evidence and proof in civil disputes arising from remote transactions, we should note that the evidence verifiability and the parties' trust in evidence sources considered in the above work are of paramount importance.

It seems that the procedures for recognizing certain evidence as admissible in disputes over distant transactions should be regulated at the level of law. In this case, the parties should have an opportunity to agree upon the method of certain facts confirmation within the limits established by law. The legislator should set these limits taking into account the balance of interests of the parties to a distant transaction, as well as the probable information asymmetry.

Another important aspect of consideration of disputes arising from distant transactions refers to the court's application of a particular standard of proof and peculiarities of distribution of the burden of proof.

The current procedural legislation does not contain a definition of the standard of proof. In the legal literature there are different viewpoints regarding the expediency of legislative stipulation of this legal construct (Tokareva, 2023).

Meanwhile, the analysis of judicial practice shows that in resolving disputes courts develop approaches to using certain standards of proof in relation to various categories of disputes ("balance of probabilities", "clear and convincing evidence", "clear and convincing evidence")[14] .

It seems that for disputes on remote transactions, in terms of proving the facts based on interaction using digital technologies, a special standard of proof should be developed, taking into account the legal status of the parties to the transaction.

This issue requires special research. In terms of setting a problem for discussion, it can be proposed that the obligation to provide digital evidence should be imposed on the party that keeps information or is the closest to the one who keeps it. The same party should have the burden of proving the document immutability in case the other party alleges that it was distorted. The party that is the keeper of evidence in the digital environment should be subject to the "clear and convincing evidence" standard for the circumstances it refers to. For the other party, the "balance of probabilities" standard is sufficient.

---

[14] Ruling of the Judicial Division on economic disputes of the Supreme Court of the Russian Federation No. 308-ES17-6757(2, 3) of 06.08.2018 in case No. A22-941/2006. SPS KonsultantPlyus. ссылку; Ruling of the Judicial Division on economic disputes of the Supreme Court of the Russian Federation No. 305-ES16-18600(5–8) of 30.09.2019 in case No. A40-51687/2012. SPS KonsultantPlyus. https://clck.ru/36brxP

3.3. Utilization of the potential of artificial intelligence, smart contracts in remote interaction of participants of contractual relations

Certain business spheres carry risks and inconveniences for key participants that could be solved by utilizing the opportunities inherent in digital technologies but not fully used in practice.

As an example, let us take construction of various commercially beneficial facilities (apartment buildings, hotels, business centers, etc.) The key participants in a construction project may include a developer, a builder, a designer, a technical customer, a general contractor, investors, insurers, a credit organization, etc.

At the moment, the relations between the construction project participants are built within bilateral contractual obligations, approximately as follows:

– developer – designer;
– developer – investor(s);
– developer – general contractor;
– general contractor– contractor;
– general contractor– supplier;
– developer – technical customer;
– developer – credit organization;
– developer – insurance organization.

It is important for project participants to obtain objective and verified data:

– at the initial stage – regarding the state of the real estate market, supply and demand for similar objects, market trends, as well as the cost of construction and prospects for its change;

– at subsequent stages – regarding market changes in the parameters initially included in the business model, as well as the degree of the object readiness in relation to the established schedule.

The current practice shows that the collection, verification and analysis of information are carried out by different entities, which negatively affects the investment climate.

For example, at the very initial stage the developer should assess the prospects of the territory development, decide on the concept of the future construction, conduct economic analysis, including forecasting the return on investment, select the appropriate land plot, and ensure the development of project documentation.

At the stage of obtaining bank funding, all parameters included in the business model are checked and evaluated by the credit organization, which takes additional steps to obtain objective data from independent sources and uses its own methods to assess the risks of the project. Investors, when deciding to invest in a project, are also interested in obtaining objective information and correctly assessing the project potential.

Later, at the construction stage, all participants are directly interested in having reliable information about the project progress and the impact of the changes affecting the parameters laid out in the business model.

When collecting and analyzing information, none of the subjects can be sure of its objectivity, the correctness of its assessment, and the adequacy of the risk taken. This creates uncertainty among investors about the project payback; hence a prolonged consideration of the credit application by the credit organization and the establishment of credit terms based on conservative approaches aimed at hedging risks, including the risk of unreliable information.

These circumstances lead to the fact that entrepreneurs in the construction sector eventually reject interesting ideas, as it is difficult to prove the prospects of payback and income to investors and the lending bank.

A similar situation occurs in other areas where the business process is based on industrial and financial integration with a large number of entities. As it is noted, a supply chain financing has recently emerged – a financial activity derived from the production chain of the real economy. The application of smart contracts in the supply chain is proposed. This will solve the problem of access to credit resources for small and medium-sized enterprises (Zhang et al., 2021). The supply chain and all its logical relationships must be fully mapped to the blockchain network to ensure that each one is transparent, authentic and verifiable (Dietrich et al., 2020).

Of interest is the research conducted by Will Serrano, who presents the Validation and Verification (V & V) model, an AI-based data marketplace that consists of three levels of verification, each having value for certain project participants. Silver verification, for example, has value for insurers in particular. It involves analyzing data to find deviations from a range or a value-added rule. The third level – Gold verification: data prediction based on multiple Artificial Intelligence (AI) algorithms and Machine Learning (ML) models – is relevant to the city in general or to asset managers and city developers (Serrano, 2022).

The above allows concluding that the implementation of an informational interactive model with data verification via blockchain and smart contract will solve the problem of trust between participants in business processes with a high degree of production integration. It will also provide an opportunity for effective management and commercialization of a project or investments.

In our opinion, the legal mechanism for implementing such an informational and economic model of a project or a supply chain should imply, as an initial stage, the enshrinement of rules in public law providing for:

– developing requirements to AI for solving the above tasks;

– carrying out an expert examination of the correctness of the tasks to be performed by the AI and the recognition of the results of their solution. The expertise should be conducted with the participation of specialized state bodies (in the field of construction and supervisory bodies in the field of banking, etc.).

Relations between private law subjects can be built using the model of remote transactions. The area of such transactions will be the use of data contained in the project's information model without the right to make adjustments, delete data, etc.

A more detailed analysis of the proposed option of using remote transactions is not possible at the moment due to the lack of well-developed basic approaches even at the level of draft regulations or doctrinal provisions in this area of public law.

Conclusions

1. The development of digital technologies gives rise to new remote ways of conducting transactions, as well as provides new content to the traditional civil law procedures for contract concluding via the exchange of messages.

2. The current legislation does not single out a "remote contract" as a legal construction (model) of a civil law contract.

Meanwhile, the use of digital technologies in the remote method of interaction between the contractual relations participants generates a significant number of problems that could be solved within a special contractual construction of "remote contract" under a special legal regime.

3. The author distinguishes the following features of a "remote contract":

– the contract is concluded without personal presence of the parties at the moment of will expression at the place of the contract conclusion;

– digital technologies are used in remote interaction.

Under a special legal regime of "remote contract" the following issues should be solved, as a minimum:

– the criteria for establishing the status of the parties to the contract, while recognizing one of them as a weak party;

– the conditions of liability of the parties, including the application of the "strict" liability principle (regardless of the presence of guilt) and the limits of its application;

– who bears the risks of technological failures or hacker attacks;

– the distribution of the burden of proof between the parties.

4. Along with a "distant contract", "distant transactions" should be distinguished as a legal category.

This said, the basic concept should be that of a "distant contract", the rules of which can be extended to unilateral distant transactions.

5. A unilateral transaction may be qualified as a distant transaction if the following features are present:

– a unilateral transaction is a transaction requiring perception;

– communication of the will expression to the counterparty is carried out using digital technologies.

6. The need to single out distant transactions as a separate category is due, among other things, to a number of specific aspects that fall beyond civil law regulation. These include:

– assignment of public functions to private subjects (carriers of information on distant transactions);

– peculiarities of proof in disputes arising from remote transactions;

– using the potential of AI and smart contracts in the remote interaction of participants of contractual relations.

References

Akuzhinov, A. (2020). Transactions requiring and not requiring discernment: theoretical and practical basis for qualification. *Tsivilistika*, *6*, 124–152. (In Russ.).

Aquilina, S. J., Casino, F., Vella, M., Ellul, J., & Patsakis, C. (2021). EtherClue: Digital investigation of attacks on Ethereum smart contracts. *Blockchain: Research and Applications*, *2*(4), 100028. https://doi.org/10.1016/j.bcra.2021.100028

Belov, V. A. (2021). Smart contract: concept, legal regulation, law enforcement practice, consumer relations. *Pravo i ehkonomika*, *9*, 35–41. (In Russ.).

Chelysheva, N. Yu. (2022). Concept of legal regulation of smart contract in civil law. *Pravo i ehkonomika*, *7*, 32–36. (In Russ.).

Churilov, A. Yu. (2020). On the concept and legal nature of a smart contract. *Yurist*, *7*, 25–30. https://doi.org/10.18572/1812-3929-2020-7-25-30

Dietrich, F., Palm, D., & Louw, L. (2020). Smart contract based framework to increase transparency of manufacturing networks. *Procedia CIRP*, *91*, 278–283. https://doi.org/10.1016/j.procir.2020.02.177

Efimova, L. G. (2019). On the Concept and Legal Nature of the Electronic Form of the Transaction. *Lex Russica*, *8*, 129–137. (In Russ.) https://doi.org/10.17803/1729-5920.2019.153.8.129-137

Efimova, L. G., & Sizemova, O. B. (2019). Legal nature of a smart contract. *Banking Law*, *1*. (In Russ.). https://doi.org/10.18572/1812-3945-2019-1-21-28

Egorov, A. V. (2015). The Supreme Court has clarified the concept of a transaction. Has it become clearer? *Arbitrazhnaya praktika*, *12*, 29. (In Russ.).

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Corrias, G., Moncada, R., Cavallaro, A., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, *4*(3), 100142. https://doi.org/10.1016/j.bcra.2023.100142

Filipova, I. A. (2023). Artificial Intelligence: The Degree of Influence on Labor Relations. *Yurist*, *3*, 23–28. (In Russ.). http://dx.doi.org/10.18572/1812-3929-2023-3-23-28

Grin, O. S. (2019). Transformation of contract form requirements based on the development of digital technologies. *Actual Problems of Russian Law*, *6*, 49–57. (In Russ.). https://doi.org/10.17803/1994-1471.2019.103.6.049-057

Hsain, Ya. Ait, Laaz, N., & Mbarki, S. (2021). Ethereum's Smart Contracts Construction and Development using Model Driven Engineering Technologies: a Review. *Procedia Computer Science*, *184*, 785–790. https://doi.org/10.1016/j.procs.2021.03.097

Kennedy, G. (2023). The "Gold" Standard – China finalises the long-anticipated Standard Contract under the Personal Information Protection Law. *Computer Law & Security Review*, *49*, 105832. https://doi.org/10.1016/j.clsr.2023.105832

Kirillova, E. A. (2021). Notary transactions in electronic form: some problems of practice. *Notary*, *5*, 41–43. (In Russ.). https://doi.org/10.18572/1813-1204-2021-5-41-43

Kirli, D., Couraud, B., Robu, V., Salgado-Bravo, M., Norbu, S., Andoni, M., Antonopoulos, I., Negrete-Pincetic, M., Flynn, D., & Kiprakis, A. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, *15*, 112013. https://doi.org/10.1016/j.rser.2021.112013

Kostikova, G. V. (2022). Electronic transactions: legislative novelties. *Khozyaistvo i pravo*, *2*. (In Russ.). https://doi.org/10.18572/0134-2398-2022-2-49-59

Kozlova, M. Yu., & Sergacheva, O. A. (2022). The impact of digitalization on the form of a contract. *Tsivilist*, *1*. (In Russ.).

Kuzmina, A. V., & Lomakina, E. A. (2022). Protection of the weak party from the imposition of unfair terms of the contract concluded on the Internet. *Russian Juridical Journal*, *4*. (In Russ.). https://doi.org/10.34076/20713797_2022_4_121

Laptev, V. A., & Solovyanenko, N. I. (2022). A Distance Transaction and an Electronic Signature: The Legal Structure and the Form of Conclusion. https://doi.org/10.18572/1812-3929-2022-12-16-22

Lim, A., & Pan, E. (2021). 'Toward a Global Social Contract for Trade' – a Rawlsian approach to Blockchain Systems Design and Responsible Trade Facilitation in the New Bretton Woods era. *Journal of Responsible Technology*, *6*, 100011. https://doi.org/10.1016/j.jrt.2021.100011

Mikhaylova, A. S. (2020). On some aspects of electronic technology application in will attestation. *Notary*, *7*, 28–31. (In Russ.). https://doi.org/10.18572/1813-1204-2020-7-28-31

Ovchinnikova, Yu. S. (2022). Digitalization of insurance services: protection of the weak side of the contract and private life. *Property Relations in the Russian Federation*, *3*, 73–81. (In Russ.). http://dx.doi.org/10.24412/2072-4098-2022-3246-73-81

Philip, A. O., & Saravanaguru, R. K. (2022). Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *Journal of King Saud University – Computer and Information Sciences*, *34*(7), 4031–4046. https://doi.org/10.1016/j.jksuci.2022.06.001

Savelyev, A. I. (2016). Contract law 2.0: "smart contracts" and the beginning of the end of the classic contract law. *Civil Law Review*, *3*, 32–60. (In Russ.).

Savelyeva, T. A. (2022). Digitalization: protection of the weak side of the contract. In I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, & A. A. Shutova, *Digital Technologies and Law: collection of works of the I International Scientific and Practical Conference* (Kazan, September 23, 2022). (In 6 vol. Vol. 2, pp. 478–490). Kazan: Poznaniye Publishers of Kazan Innovative University. http://dx.doi.org/10.21202/978-5-8399-0769-0_2022_2_556

Serrano, W. (2022). Verification and Validation for data marketplaces via a blockchain and smart contracts. *Blockchain: Research and Applications*, *3*(4), 100100. https://doi.org/10.1016/j.bcra.2022.100100

Shelepina, E. A. (2021). Trends of legal regulation of electronic document flow in national civil law. *Law and Digital Economy*, *1*, 26–35 (In Russ.). http://dx.doi.org/10.17803/2618-8198.2021.11.1.026-035

Tărchilă, P., & Nagy, M. (2015). Comparative Approach of the Electronic Contract and Classical Contract, in Teaching The Content of the New Civil Code in Romania. *Procedia – Social and Behavioral Sciences*, *191*, 464–468. https://doi.org/10.1016/j.sbspro.2015.04.588

Tokareva, E. V. (2023). On the place of the "standard of proof" in the civilistic procedure. *Vestnik arbitrazhnoi praktiki*, *2*, 35–40. (In Russ.). https://clck.ru/36m8nU

Tosza, S. (2021). Internet service providers as law enforcers and adjudicators. A public role of private actors. *Computer Law & Security Review*, *43*, 105614. https://doi.org/10.1016/j.clsr.2021.105614

Tsepov, G. V., Ivanov, N. V. (2022). Towards a Civil-Law Theory of Smart Contracts. *Zakon*, *3*, 149–172. (In Russ.). https://doi.org/10.37239/0869-4400-2022-18-3-149-172

Utkin, V. V. (2022). On the legal regulation of smart contracts. *Economy and Law*, *11*, 92–98. http://dx.doi.org/10.18572/0134-2398-2022-11-92-98

Van Rompaey, L., Jønsson, R., & Jørgensen, K. E. (2022). Designing lawful machine behaviour: Roboticists' legal concerns. *Computer Law & Security Review*, *47*, 105711. https://doi.org/10.1016/j.clsr.2022.105711

Yatsenko, T. S. (2019). Problems of legal regulation of electronic wills in foreign countries. *Notary*, 7, 42–44. (In Russ.).

Zhang, TianLin, Li, JinJiang, & Jiang, Xinbo. (2021). Supply chain finance based on smart contract. *Procedia Computer Science*, *187*, 12–17. https://doi.org/10.1016/j.procs.2021.04.027

Author information

Tatyana A. Savelyeva – Cand. Sci. (Law), Associate Professor of Department of Civil Law, Novosibirsk Law Institute (branch) of Tomsk State University
Address: 7 Sovetskaya Str., 630007 Novosibirsk, Russian Federation
E-mail: sta.sd@bk.ru
ORCID ID: https://orcid.org/0009-0000-9831-665X
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1195986

Conflicts of interest

The authors declare no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – July 31, 2023
Date of approval – August 21, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:347.45/.47
EDN: https://elibrary.ru/lbzqze
DOI: https://doi.org/10.21202/jdtl.2023.46

Дистанционные способы совершения сделок с использованием цифровых технологий

Татьяна Александровна Савельева

Новосибирский юридический институт (филиал) Томского государственного университета
г. Новосибирск, Российская Федерация

Ключевые слова

баланс интересов,
блокчейн,
дистанционная сделка,
дистанционный договор,
информационные технологии,
искусственный интеллект,
право,
смарт-контракт,
цифровые технологии,
электронный документ

Аннотация

Цель: обоснование необходимости выделения новых договорных конструкций (моделей) с учетом специфики отношений, связанных с использованием дистанционного способа заключения договора посредством цифровых технологий и возможными рисками для их участников.

Методы: наряду со специально-юридическими методами основополагающим в процессе исследования стал метод критического анализа, что позволило оценить и интерпретировать основные источники и нормы гражданского права применительно к совершению дистанционных сделок, проанализировать современное состояние законодательства в этой области в контексте развивающихся процессов цифровизации и технологизации гражданско-правовых отношений.

Результаты: представлен критический анализ текущего состояния правовой регламентации дистанционных способов заключения договоров, дана их классификация. Сделан вывод о том, что развитие цифровых технологий порождает новые дистанционные способы совершения сделок, а также наполняет новым содержанием традиционные для гражданского права процедуры заключения договора. Обоснована целесообразность выделения понятия «дистанционная сделка» в качестве правовой категории в целях создания специального гражданско-правового режима, при этом базовым понятием должно являться понятие «дистанционный договор». Проанализированы отдельные виды дистанционных договоров для обоснования идеи о необходимости специальных правовых режимов в случаях, когда дистанционный способ заключения договора сочетается с использованием цифровых технологий, применение которых ставит такие проблемы, как распределение рисков технологических сбоев, хакерских атак, соблюдение баланса интересов сторон с учетом информационной асимметрии, необходимость защиты слабой стороны.

Научная новизна: предпринята попытка дать определение таких понятий, как «дистанционный договор», «дистанционная сделка», выделить их признаки. Обоснована целесообразность рассмотрения дистанционного договора в качестве самостоятельной правовой конструкции (модели) договора, в рамках которой должен быть разработан и закреплен специальный правовой режим, который может быть распространен на односторонние дистанционные сделки. Сформулированы проблемы правового регулирования, обусловленные использованием информационных технологий, а также предложены правовые конструкции для их решения.

Практическая значимость: сделанные выводы и предложения могут быть использованы как в договорной практике участниками гражданского оборота, так и для нормативного закрепления понятия и признаков «дистанционного договора», «дистанционной сделки», создания специального правового режима с учетом специфики, порождаемой использованием цифровых технологий.

Для цитирования

Савельева, Т. А. (2023). Дистанционные способы совершения сделок с использованием цифровых технологий. *Journal of Digital Technologies and Law*, *1*(4), 1058–1086. https://doi.org/10.21202/jdtl.2023.46

Список литературы

Акужинов, А. (2020). Сделки, требующие и не требующие восприятия: теоретическое и практическое основание квалификации. *Цивилистика*, *6*, 124–152. https://www.elibrary.ru/hhnnis

Белов, В. А. (2021). Смарт-контракт: понятие, правовое регулирование, правоприменительная практика, потребительские отношения. *Право и экономика*, *9*, 35–41. https://www.elibrary.ru/zcbdhr

Гринь, О. С. (2019). Трансформации требований к форме договоров с учетом развития цифровых технологий. *Актуальные проблемы российского права*, *6*, 49–57. EDN: https://www.elibrary.ru/whwjyc. DOI: https://doi.org/10.17803/1994-1471.2019.103.6.049-057

Егоров, А. В. (2015). Верховный суд разъяснил понятие сделки. Наступила ли ясность? *Арбитражная практика*, *12*, 29. https://www.elibrary.ru/wmlhlv

Ефимова, Л. Г. (2019). Еще раз о понятии и правовой природе электронной формы сделки. *Lex russica*, *8*, 129–137. EDN: https://www.elibrary.ru/evaoxo. DOI: https://doi.org/10.17803/1729-5920.2019.153.8.129-137

Ефимова, Л. Г., Сиземова, О. Б. (2019). Правовая природа смарт-контракта. *Банковское право*, *1*. EDN: https://www.elibrary.ru/yvaxlv. DOI: https://doi.org/10.18572/1812-3945-2019-1-21-28

Кириллова, Е. А. (2021). Нотариальные сделки в электронной форме: некоторые проблемы практики. *Нотариус*, *5*, 41–43. EDN: https://www.elibrary.ru/uvzbuj. DOI: https://doi.org/10.18572/1813-1204-2021-5-41-43

Козлова, М. Ю., Сергачева, О. А. (2022). Влияние цифровизации на форму договора. *Цивилист*, *1*. https://www.elibrary.ru/edwlwo

Костикова, Г. В. (2022). Электронные сделки: новеллы законодательства. *Хозяйство и право*, *2*, 49–59. EDN: https://elibrary.ru/azafwm. DOI: https://doi.org/10.18572/0134-2398-2022-2-49-59

Кузьмина, А. В., Ломакина, Е. А. (2022). Защита слабой стороны от навязывания несправедливых условий договора, заключаемого в сети Интернет. *Российский юридический журнал*, *4*. EDN: https://elibrary.ru/zcrhpw. DOI: https://doi.org/10.34076/20713797_2022_4_121

Лаптев, В. А., Соловяненко, Н. И. (2022). Дистанционная сделка и электронная подпись: правовая конструкция и форма заключения. *Юрист*, *12*, 16–22. EDN: https://elibrary.ru/qpaihf. DOI: https://doi.org/10.18572/1812-3929-2022-12-16-22

Михайлова, А. С. (2020). К вопросу об отдельных аспектах применения электронных технологий в процессе удостоверения завещаний. *Нотариус*, *7*, 28–31. EDN: https://elibrary.ru/onmssw. DOI: https://doi.org/10.18572/1813-1204-2020-7-28-31

Овчинникова, Ю. С. (2022). Цифровизация страховых услуг: защита слабой стороны договора и частной жизни. *Имущественные отношения в Российской Федерации*, *3*, 73–81. EDN: https://elibrary.ru/sywrgk. DOI: http://dx.doi.org/10.24412/2072-4098-2022-3246-73-81

Савельев, А. И. (2016). Договорное право 2.0: «умные» контракты как начало конца классического договорного права. *Вестник гражданского права*, *3*, 32–60. https://elibrary.ru/whffcx

Савельева, Т. А. (2022). Цифровизация: защита слабой стороны договора. В сб. И. Р. Бегишев, Е. А. Громова, М. В. Залоило, И. А. Филипова, А. А. Шутова, *Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции* (г. Казань, 23 сентября 2022 г.) (в 6 т. Т. 2, с. 478–490). Казань: Изд-во «Познание» Казанского инновационного университета. EDN: https://elibrary.ru/jsixfm. DOI: http://dx.doi.org/10.21202/978-5-8399-0769-0_2022_2_556

Токарева, Е. В. (2023). О месте «стандарта доказывания» в цивилистическом процессе. *Вестник арбитражной практики*, *2*, 35–40. https://clck.ru/36m8nU

Уткин, В. В. (2022). К вопросу о правовом регулировании смарт-контрактов. *Хозяйство и право*, *11*, 92–98. http://dx.doi.org/10.18572/0134-2398-2022-11-92-98

Филипова, И. А. (2023). Искусственный интеллект: горизонт влияния на трудовые правоотношения. *Юрист*, *3*, 23–28. http://dx.doi.org/10.18572/1812-3929-2023-3-23-28

Цепов, Г. В., Иванов, Н. В. (2022). К цивилистической теории смарт-контрактов. *Закон*, *3*, 149–172. http://dx.doi.org/10.37239/0869-4400-2022-18-3-149-172

Челышева, Н. Ю. (2022). Концепция правового регулирования смарт-контракта в гражданском праве. *Право и экономика*, *7*, 32–36. https://elibrary.ru/mjmzfn

Чурилов, А. Ю. (2020). К проблеме понятия и правовой природы смарт-контракта. *Юрист*, *7*, 25–30. EDN: https://elibrary.ru/bouxik. DOI: https://doi.org/10.18572/1812-3929-2020-7-25-30

Шелепина, Е. А. (2021). Тенденции правового регулирования электронного документооборота в национальном гражданском праве. *Право и цифровая экономика*, *1*, 26–35. EDN: https://elibrary.ru/qhhhgi. DOI: http://dx.doi.org/10.17803/2618-8198.2021.11.1.026-035

Яценко, Т. С. (2019). Проблемы правового регулирования электронных завещаний в зарубежных странах. *Нотариус*, *7*, 42–44. https://elibrary.ru/idsjmj

Aquilina, S. J., Casino, F., Vella, M., Ellul, J., & Patsakis, C. (2021). EtherClue: Digital investigation of attacks on Ethereum smart contracts. *Blockchain: Research and Applications*, *2*(4), 100028. https://doi.org/10.1016/j.bcra.2021.100028

Dietrich, F., Palm, D., & Louw, L. (2020). Smart contract based framework to increase transparency of manufacturing networks. *Procedia CIRP*, *91*, 278–283. https://doi.org/10.1016/j.procir.2020.02.177

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Corrias, G., Moncada, R., Cavallaro, A., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, *4*(3), 100142, https://doi.org/10.1016/j.bcra.2023.100142

Hsain, Ya. Ait, Laaz, N., & Mbarki, S. (2021). Ethereum's Smart Contracts Construction and Development using Model Driven Engineering Technologies: a Review. *Procedia Computer Science*, *184*, 785–790, https://doi.org/10.1016/j.procs.2021.03.097

Kennedy, G. (2023). The "Gold" Standard – China finalises the long-anticipated Standard Contract under the Personal Information Protection Law. *Computer Law & Security Review*, *49*, 105832. https://doi.org/10.1016/j.clsr.2023.105832

Kirli, D., Couraud, B., Robu, V., Salgado-Bravo, M., Norbu, S., Andoni, M., Antonopoulos, I., Negrete-Pincetic, M., Flynn, D., & Kiprakis, A. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, *15*, 112013. https://doi.org/10.1016/j.rser.2021.112013

Lim, A., & Pan, E. (2021). 'Toward a Global Social Contract for Trade' – a Rawlsian approach to Blockchain Systems Design and Responsible Trade Facilitation in the New Bretton Woods era. *Journal of Responsible Technology*, *6*, 100011. https://doi.org/10.1016/j.jrt.2021.100011

Philip, A. O., & Saravanaguru, R. K. (2022). Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *Journal of King Saud University – Computer and Information Sciences*, *34*(7), 4031–4046. https://doi.org/10.1016/j.jksuci.2022.06.001

Serrano, W. (2022). Verification and Validation for data marketplaces via a blockchain and smart contracts. *Blockchain: Research and Applications*, *3*(4), 100100. https://doi.org/10.1016/j.bcra.2022.100100

Tărchilă, P., & Nagy, M. (2015). Comparative Approach of the Electronic Contract and Classical Contract, in Teaching The Content of the New Civil Code in Romania. *Procedia – Social and Behavioral Sciences*, *191*, 464–468. https://doi.org/10.1016/j.sbspro.2015.04.588

Tosza, S. (2021). Internet service providers as law enforcers and adjudicators. A public role of private actors. *Computer Law & Security Review*, *43*, 105614. https://doi.org/10.1016/j.clsr.2021.105614

Van Rompaey, L., Jønsson, R., & Jørgensen, K. E. (2022). Designing lawful machine behaviour: Roboticists' legal concerns. *Computer Law & Security Review*, *47*, 105711. https://doi.org/10.1016/j.clsr.2022.105711

Zhang, TianLin Li, JinJiang, & Jiang, Xinbo. (2021). Supply chain finance based on smart contract. *Procedia Computer Science*, *187*, 12–17. https://doi.org/10.1016/j.procs.2021.04.027

Сведения об авторе

Савельева Татьяна Александровна – кандидат юридических наук, доцент кафедры гражданского права, Новосибирский юридический институт (филиал) Томского государственного университета
Адрес: 630007, Российская Федерация, г. Новосибирск, ул. Советская, 7
E-mail: sta.sd@bk.ru
ORCID ID: https://orcid.org/0009-0000-9831-665X
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1195986

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.27.41 / Сделки
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 31 июля 2023 г.
Дата одобрения после рецензирования – 21 августа 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.47

Digital Transformations of the South African Legal Landscape

William Manga Mokofe

High Court of South Africa
East London, South Africa

Keywords

artificial intelligence,
cybercrime,
digital technologies,
intellectual property right,
judicial practice,
law,
legislation,
online dispute resolution,
personal data protection,
South Africa

Abstract

Objective: South Africa is a country with great potential for intensive development due to the active growth and adoption of digital technologies. The rapidly emerging digital landscape is transforming the legal framework, which in turn influences the digital environment. This transformative relationship determined the focus of the research, which is to identify the legal system adaptability under dynamic changes, as well as the legal landscape evolution under digitalization and technological progress.

Methods: the study of the changing legal landscape required an interdisciplinary approach that combines legal analysis with ideas from sociology, economics, etc. In doing so, the formal-legal method was used to examine the key legal instruments shaping South Africa's digital environment and providing the opportunities and challenges of the interaction between digital technologies and South African law.

Results: the paper provides insights into how the South African legal system is addressing digital challenges; assesses the integration of digital innovations into the legal system; highlights the transformative impact of digital technologies on traditional legal processes, including collecting evidence, dispute resolution and access to justice. Finally, it evaluates the role of digital technologies in making legal processes more efficient.

Scientific novelty: the study contributes to the ongoing debate on the complex relationship between digital technologies and South African law. It shows how South African law is coping with digital complexities

and substantiates new insights into the transformation of the traditional legal paradigm as a result of digitalization, as well as its implications for legal proceedings and access to justice. By delving into the adaptations, challenges and innovations arising at the intersection of law, technologies and digitalization, insights are gained into how South African law navigates the dynamic digital landscape.

Practical significance: adapting the legal landscape to digitalization and technological advances is critical to ensure rapid technological progress. It also requires collaboration between government agencies, civil society, experts in law and technology. The study provides valuable recommendations and suggestions for policymakers, legal practitioners and stakeholders shaping South Africa's legal ecosystem. The author addresses the challenges of ensuring personal data privacy, enhancing electronic interactions, and countering cybercrime. The importance of introducing technological achievements while maintaining robust legal safeguards is emphasized.

For citation

Mokofe, W. M. (2023). Digital Transformations of the South African Legal Landscape. *Journal of Digital Technologies and Law, 1*(4), 1087–1104. https://doi.org/10.21202/jdtl.2023.47

Contents

Introduction

In the modern landscape, the intricate interplay between digital technologies and the legal framework has ushered in a new era of challenges and opportunities, nowhere more evident than in the context of South Africa. The rapid evolution of digital technologies has been reshaping societies, economies, and governance structures, fundamentally altering the way people communicate, transact, and interact (Mokofe & van Eck, 2021). This transformative

impact has prompted a compelling need to scrutinize the adaptability of legal systems in the face of these dynamic changes.

The overarching aim of this exploration is to delve into how South African law has responded and adapted to the rapidly advancing digital technologies while evaluating the broader implications of this adaptation. The interconnection of these realms is not merely coincidental; rather, it reflects a symbiotic relationship wherein the legal framework seeks to regulate and harness the potential of digital technologies, and in turn, digital technologies challenge the legal norms that have been traditionally established (Adams & Adeleke, 2020).

The digital landscape encompasses a wide array of technologies, ranging from ubiquitous smartphones and the omnipresent Internet to more specialized domains like blockchain, artificial intelligence, and the Internet of Things (IoT). Each of these technologies brings its own set of opportunities and complexities, intertwining with various aspects of law, from data protection and privacy to intellectual property and cybercrime (Mokofe & van Eck, 2022; Swales, 2021). Consequently, exploring this landscape necessitates a multidisciplinary approach that combines legal analysis with insights from technology, sociology, economics, and beyond.

One of the primary focal points of this inquiry is the legal frameworks that have been established to govern the digital sphere in South Africa. The enactment of laws such as the Protection of Personal Information Act (POPIA)[1] and the Electronic Communications and Transactions Act (ECTA)[2] exemplifies the nation's proactive efforts to provide legal guidelines for the digital age. These statutes seek to ensure that the proliferation of digital technologies is not accompanied by the erosion of individual rights, data privacy, and security.

Moreover, as the digital landscape knows no geographical boundaries, it presents unique jurisdictional challenges. Cybercrime, often orchestrated from distant locations, forces legal systems to confront the complexities of transnational law enforcement and cooperation (Mtuze, 2022; Swales, 2022). This global interconnectedness highlights the need for international collaboration, as well as the development of legal instruments that can effectively tackle the novel challenges brought forth by technology.

Beyond its regulatory aspects, digital transformation is reshaping conventional legal processes. The introduction of digital evidence, the utilization of Artificial Intelligence (AI) legal research, and the rise of online dispute-resolution platforms are altering the very fabric of litigation and dispute resolution (De Sousa et al., 2021). These shifts bring efficiency gains but also demand a critical evaluation of their impact on traditional notions of justice and due process.

---

1 Copyright Amendment Act, No. 9 of 2019.

2 Electronic Communications and Transactions Act, No. 25 of 2002.

The integration of digital technologies within the legal framework of South Africa encapsulates a multifaceted discourse that bridges technology, law, and society (Botha et al., 2017). This exploration seeks to traverse this evolving landscape, shedding light on the intricate relationship between legal norms and technological advancements. By delving into the adaptations, challenges, and innovations that emerge at this intersection, this study aims to contribute to a comprehensive understanding of how South African law navigates the dynamic terrain of the digital age.

1. Adaptation of South African law to rapidly advancing digital technologies

The convergence of digital technologies and the legal landscape in South Africa has led to a complex and evolving relationship, necessitating a responsive and adaptable legal framework. As digital technologies continue to reshape traditional norms and modes of operation, South African law has undergone a series of significant adaptations to address the multifaceted challenges and opportunities presented by this paradigm shift (Naude & Papadopoulos, 2016). These dynamic adaptions are discussed below.

2. Data protection and privacy

One of the most pronounced adaptations has been in the realm of data protection and privacy. The enactment of the Protection of Personal Information Act (POPIA)[3] stands as a seminal response to the increasing digitization of personal information. POPIA establishes a comprehensive legal framework for the collection, processing, and storage of personal data, aiming to ensure individuals' rights are upheld in the digital age. By imposing stringent obligations on data controllers and processors, the law seeks to strike a balance between technological innovation and safeguarding personal privacy.

The accelerated integration of digital technologies into everyday life has significantly impacted data protection and privacy concerns. Foremost among South Africa's legal adaptations to these evolving challenges is the enactment of the POPIA. With the escalating digitization of personal information and the proliferation of online data exchanges, POPIA serves as a pivotal response that aims to harmonize individual rights and technological advancements in the digital age.

POPIA's establishment represents a comprehensive effort to create a legal framework capable of regulating the collection, processing, and storage of personal data while preserving individuals' privacy (Adams & Adeleke, 2020; Bronstein, 2022). In essence, it underscores the growing recognition of data as a valuable commodity, the safeguarding of which requires robust legal mechanisms. The Act encapsulates an assortment of provisions that delineate the rights of data subjects and the responsibilities of data controllers and processors (Naude & Papadopoulos, 2016).

[3] Protection of Personal Information Act, No. 4 of 2013.

By placing stringent obligations on entities handling personal data, the legislation seeks to strike a delicate equilibrium between facilitating innovation and protecting individuals' privacy (Malgieri & Comandé, 2017). Through its provisions, POPIA enforces transparency and accountability by mandating data controllers obtain explicit consent for data processing, disclose data usage, and implement adequate security measures to prevent breaches.

Furthermore, POPIA's establishment signifies a response to the global trend of data protection regulations, emphasizing South Africa's commitment to aligning its legal landscape with international standards (Adams & Adeleke, 2020). The Act's introduction has far-reaching implications for businesses operating in the digital sphere, requiring them to revise their data management practices and establish mechanisms for compliance.

Further, the enactment of POPIA represents a crucial adaptation of South African law to address the burgeoning concerns surrounding data protection and privacy in an increasingly digitized world. By providing a robust legal framework that sets the tone for responsible data management and privacy preservation, the legislation endeavours to harmonize technological innovation with fundamental rights.

3. Cybercrime legislation

In, recognition of the escalating threat of cybercrime, South African law has been reshaped to encompass a range of offences and penalties related to digital crimes. The Cybercrimes Act[4] represents a notable milestone, criminalizing a wide array of activities including hacking, identity theft, and cyberbullying. This legislation underscores the recognition of the unique challenges posed by digital offences and the necessity to provide a legal framework that can effectively combat such crimes while protecting individuals' digital rights.

The surge in cyber threats has spurred a critical overhaul of South African law to tackle the burgeoning menace of digital crimes. As digital technologies continue to advance, South African lawmakers recognized the pressing need to adapt the legal framework to effectively address cybercrime. This evolving landscape prompted the enactment of the Cybercrimes Act, signifying a pivotal step toward enhancing the nation's capability to combat a spectrum of digital offences.

The Cybercrimes Act, a significant legislative development, serves as an instrumental response to the multifaceted nature of cybercrime. With its comprehensive approach, the Act marks a departure from traditional legal paradigms by specifically criminalizing a wide spectrum of cyber offences. Activities ranging from hacking and identity theft to cyberbullying are brought under the purview of the law, underlining the South African legal system's resolve to adapt to contemporary challenges (Roos, 2020).

[4] Cybercrimes Act, No. 19 of 2020.

By encompassing a diverse array of cyber offences, the Act reflects a nuanced understanding of the evolving digital threat landscape and the necessity for a multifaceted legal response (Malgieri & Comandé, 2017). This legislation recognizes that cybercrime extends beyond financial fraud to encompass activities that compromise individuals' privacy, safety, and well-being in the digital realm. As such, the Act aligns with international trends in cybercrime legislation, demonstrating South Africa's commitment to fostering cybersecurity (de Bruyn, 2014).

The introduction of the Cybercrimes Act underscores a strategic shift in legal reasoning, acknowledging the distinctive challenges and complexities posed by digital offences. This legislation not only seeks to penalize perpetrators but also reinforces the need to secure individuals' digital rights (Van Niekerk, 2018). By outlining penalties commensurate with the severity of offences, the Act aims to deter potential wrongdoers while providing a solid foundation for law enforcement agencies to effectively combat cybercrime.

More so, the adoption of the Cybercrimes Act exemplifies South Africa's proactive approach to shaping its legal framework to counter the escalating threat of digital crimes. Through its comprehensive scope, the Act underscores the dynamic nature of cyber threats and the necessity for a robust legislative response. As the digital landscape evolves, the Act lays the groundwork for safeguarding individuals' digital rights and fostering a secure digital environment (Van Niekerk , 2017).

4. Electronic communications transaction

The ECTA embodies South Africa's response to the digital transformation of commercial activities and interactions. By providing legal recognition to electronic signatures, contracts, and communications, ECTA facilitates the growth of e-commerce and electronic transactions while ensuring their validity and enforceability. This adaptation acknowledges the increasing prevalence of digital interactions and endeavours to provide legal certainty in an ever-evolving digital landscape.

In the wake of the digital revolution reshaping commercial interactions and transactions, South African law has taken a proactive stance through the Electronic ECTA. This legislation represents a comprehensive response to the challenges and opportunities posed by the digital transformation of commerce, signaling the nation's commitment to fostering a legally sound environment for electronic interactions.

The ECTA's enactment underscores the realization that traditional modes of commerce have evolved with the integration of digital technologies. By extending legal recognition to electronic signatures, contracts, and communications, the Act embraces the burgeoning growth of e-commerce while ensuring that electronic transactions remain valid, enforceable, and legally binding (Staunton & De Stadler, 2019). This recognition is a pivotal aspect in addressing the unique characteristics of the digital age, where the physical presence of individuals is not essential for commercial engagements.

The ECTA's provisions resonate with the changing dynamics of the modern business landscape. The Act's emphasis on legal certainty ensures that parties engaged in electronic transactions have a clear understanding of their rights, obligations, and the legal consequences of their actions. This legal clarity is instrumental in promoting trust and confidence in online interactions, mitigating uncertainties that may otherwise hinder the growth of e-commerce and digital transactions.

Furthermore, the ECTA's adaptation reflects South Africa's commitment to aligning its legal framework with international norms. As globalization accelerates, the harmonization of legal principles related to electronic transactions contributes to fostering cross-border commerce and international trade relationships.

The introduction of the ECTA not only underscores the legal framework's adaptability but also its resilience in embracing the rapid evolution of digital technologies. By addressing the intricacies of electronic interactions and transactions, the Act lays the foundation for a robust framework that facilitates the continued growth of e-commerce while upholding legal principles.

The Electronic Communications and Transactions Act stands as a defining response to the digital transformation of commerce, encapsulating South Africa's proactive approach to adapting its legal framework. Through its recognition of electronic signatures, contracts, and communications, the ECTA bridges the gap between traditional legal norms and the ever-evolving digital landscape, promoting legal certainty and trust in electronic interactions.

5. Intellectual property and digital innovation

The convergence of digital technologies and intellectual property rights has necessitated a recalibration of copyright, patent, and trademark laws. The Copyright Amendment, for instance, addresses challenges posed by the digital reproduction and distribution of creative works. Balancing the interests of creators, innovators, and the public, the law seeks to stimulate digital innovation while safeguarding intellectual property rights.

The fusion of digital technologies and the realm of intellectual property (IP) has engendered a fundamental re-evaluation of existing legal frameworks, including copyright, patent, and trademark laws. As digital platforms become central to the creation, dissemination, and consumption of creative works and innovative ideas, South African law has embarked on a recalibration journey to align IP protection with the unique dynamics of the digital age.

One of the notable instances of this recalibration is witnessed in the Copyright Amendment. In recognizing the challenges posed by digital reproduction and distribution of creative works, this legislation illustrates the legal system's acknowledgement of the intricate interplay between digital technologies and copyright protection (Dove & Chen, 2020). The Act addresses concerns related to the unauthorized duplication and dissemination of digital content, establishing mechanisms to curb the infringement of authors' rights in the digital sphere.

Central to the Act's approach is the aspiration to strike a delicate balance between the competing interests of creators, innovators, and the wider public. By enhancing the scope of fair use provisions, the law accommodates transformative uses of copyrighted material, fostering digital innovation and creativity. The Act, therefore, encapsulates a nuanced understanding that the traditional copyright paradigm requires adaptation to accommodate the rapidly evolving modes of content consumption and creation enabled by digital technologies.

Beyond copyright, the recalibration extends to patent and trademark laws, as digital innovation often transcends traditional boundaries. The rise of software and business methods patents, for instance, has prompted legal considerations that challenge conventional patent doctrines (Talkmore, 2022). Likewise, the evolving nature of digital trademarks necessitates a re-examination of trademark registration processes and the protection of online brands in an increasingly global digital landscape.

In essence, the recalibration of IP laws exemplifies South Africa's proactive response to the dynamic synergy between digital technologies and creative expression. The legal adaptations embodied in the Copyright Amendment Act underscore the nation's commitment to fostering an environment conducive to digital innovation and creativity while safeguarding the rights of content creators and innovators.

Further, the convergence of digital technologies and intellectual property rights necessitates a comprehensive legal recalibration that navigates the intricate terrain between creativity, innovation, and digital advancements. By addressing challenges brought forth by digital reproduction, distribution, and transformation of creative works, South African law strives to cultivate an ecosystem that stimulates digital innovation while preserving the integrity of intellectual property rights.

6. Jurisdictional and enforcement challenges

As digital technologies transcend geographical borders; South African law has encountered jurisdictional challenges in addressing transnational digital offences. Ensuring effective enforcement against cybercriminals operating from foreign jurisdictions requires international collaboration, extradition treaties, and a nuanced approach to digital evidence collection and preservation.

In an increasingly interconnected world driven by digital technologies, South African law faces a complex array of jurisdictional and enforcement challenges when dealing with transnational digital offences. As cybercriminal activities span geographical boundaries with ease, the limitations of traditional legal frameworks have become apparent, necessitating an adaptive response to the evolving nature of digital crime.

The digital landscape is characterized by a borderless nature, enabling cybercriminals to exploit vulnerabilities from remote locations while causing considerable harm across jurisdictions (Van Niekerk, 2018). This has raised significant jurisdictional concerns, as South African law enforcement agencies grapple with the dilemma of prosecuting offenders beyond their national borders.

The solution to this predicament lies in international collaboration. Ensuring the effective enforcement of South African law against cybercriminals operating from foreign jurisdictions hinges upon forging robust partnerships with other nations. Extradition treaties play a pivotal role in enabling the apprehension and extradition of cybercriminals to face justice within South Africa's legal framework. These treaties provide the necessary legal foundation to overcome jurisdictional barriers that hinder the prosecution of transnational digital offences.

Central to the enforcement challenge is the preservation and collection of digital evidence. Digital evidence is inherently volatile and easily manipulable, requiring a meticulous and technologically informed approach to ensure its integrity and admissibility in legal proceedings. This entails a nuanced understanding of data preservation techniques, data privacy laws, and international protocols to guarantee the legitimacy of evidence presented before the courts.

Furthermore, the enforcement of South African law in the realm of transnational digital offences necessitates a comprehensive understanding of international legal instruments such as the Budapest Convention on Cybercrime. This convention serves as a guiding framework for international cooperation in investigating and prosecuting cybercrimes, emphasizing the importance of harmonizing legal approaches across nations[5].

The realm of transnational digital offences presents South African law with multifaceted jurisdictional and enforcement challenges. As digital technologies transcend geographical boundaries, effective response demands international collaboration, (Dove & Chen, 2020) extradition treaties, and adept evidence-collection techniques. These adaptations in legal enforcement underscore the need to address the borderless nature of cybercrime while navigating the intricacies of international law and digital evidence preservation.

7. Evolving legal processes

The integration of digital technologies has also prompted adaptations in traditional legal processes. Courts now grapple with issues related to digital evidence, electronic discovery, and the utilization of Artificial Intelligence (AI) in legal research. The evolution of online dispute resolution platforms aims to expedite the resolution of disputes while catering to the changing dynamics of digital interactions.

[5] Council of Europe. (2001). Convention on Cybercrime. https://clck.ru/36cr32

The seamless integration of digital technologies into various aspects of society has catalyzed profound changes in traditional legal processes. As the legal landscape adapts to the digital era, South African courts find themselves at the crossroads of innovation, grappling with multifaceted challenges and opportunities arising from the infusion of technology into their proceedings.

One notable aspect of this transformation is the treatment of digital evidence. The proliferation of digital interactions has necessitated a re-evaluation of evidence collection, preservation, and presentation. Courts are now tasked with understanding the intricacies of digital forensics and ensuring the integrity and admissibility of electronic evidence while upholding the principles of due process (Swales, 2018). This entails a delicate balance between embracing technology's efficiency and safeguarding the fairness of legal proceedings.

Electronic discovery, often referred to as e-discovery, has become a cornerstone of contemporary litigation. The digitization of vast amounts of data demands efficient and systematic methods for identifying, collecting, and presenting evidence. This shift has prompted legal professionals to engage with technological tools and platforms that facilitate the efficient management of digital evidence and streamline the discovery process.

Furthermore, the utilization of AI in legal research introduces a transformative dimension to legal scholarship and decision-making. AI-driven algorithms analyze vast datasets, facilitating rapid legal research, precedent analysis, and case law review. This augmentation of legal research with AI expedites information retrieval, enhances the identification of relevant legal principles, and supports more informed legal arguments.

The digitization of legal processes has also given rise to the evolution of online dispute resolution (ODR) platforms. These platforms leverage digital technologies to provide efficient and accessible mechanisms for resolving disputes (Kahungi, 2022). ODR platforms cater to the changing dynamics of digital interactions, enabling parties to engage in resolution processes without the constraints of physical presence. This alignment with the digital age aims to expedite the resolution of disputes while accommodating the realities of contemporary communication.

The integration of digital technologies into traditional legal processes is emblematic of the dynamic evolution of the legal landscape. Courts, legal professionals, and litigants alike navigate the challenges and opportunities presented by digital evidence, electronic discovery, AI-driven research, and online dispute resolution. As South African legal processes adapt to the digital era, the potential for efficiency gains and enhanced access to justice is coupled with the imperative to ensure due process and the preservation of legal rights.

Conclusion

In summation, the intricate process of adapting South African law to the rapid advancement of digital technologies emerges as an ongoing endeavour that traverses a delicate equilibrium between promoting technological advancement and preserving the fundamental rights and collective interests of individuals and society as a whole. This adaptive journey within the legal landscape reflects a conscientious effort to harmonize the ever-evolving digital realm with established legal principles, constituting a dynamic interplay that shapes the contours of the nation's legal framework.

The responsive nature of this evolving legal framework underscores the nation's commitment to ensuring that the integration of digital technologies aligns harmoniously with its societal values and individual rights. This commitment finds manifestation through a multifaceted approach that encompasses diverse areas of law, all of which have been recalibrated to address the novel challenges presented by the digital age. The multifarious components of this responsive legal architecture are epitomized by pivotal areas such as data protection, cybercrime legislation, electronic transactions, intellectual property, and jurisdictional considerations.

At the forefront, the comprehensive data protection initiatives underscore profound respect for the privacy and personal autonomy of individuals in the digital era (Bester, 2023). The implementation of stringent regulations ensures that the vast repositories of personal data harnessed by digital technologies are handled with responsibility and that the rights of individuals are preserved even as data-driven innovations surge ahead. Concurrently, the enactment of cybercrime legislation reflects a proactive stance in safeguarding the digital sphere from nefarious activities, thereby protecting both the technological ecosystem and the citizens who inhabit it (Bester, 2023).

The legal response to electronic transactions signifies South Africa's commitment to nurturing a thriving digital economy. By validating electronic signatures, contracts, and communications, the law emboldens entrepreneurs and businesses to harness the potential of e-commerce, thereby fostering economic growth while ensuring the enforceability and legality of digital transactions.

Moreover, the recalibration of intellectual property laws emphasizes an understanding of the nuanced relationship between creativity, innovation, and technological progression. By balancing the interests of creators, innovators, and the broader public, these adaptations foster a conducive environment for both digital innovation and the protection of intellectual property rights, reflecting an intricate understanding of the dual imperatives of progress and protection.

Equally significant are the jurisdictional adaptations that acknowledge the boundaryless nature of digital operations. The legal system's responsiveness to cross-border cybercrimes underscores its determination to navigate the challenges posed by global connectivity and the necessity to uphold justice in a realm devoid of conventional geographical limitations.

This adaptive legal approach signifies a commitment to seamlessly assimilating the digital age into the legal landscape while preserving its relevance and effectiveness. Nevertheless, as digital technologies continue to advance, new vistas of challenges and opportunities are set to emerge. The adaptive journey of South African law, therefore, remains an ongoing endeavour that demands unwavering vigilance. The legal system is poised to address emerging complexities and transformations with the same responsive spirit, ensuring that the rights, aspirations, and well-being of the nation's populace are both safeguarded and propelled forward in a digital landscape marked by continuous evolution.

In essence, the adaptation of South African law to digital technologies is not a destination but a dynamic process, a continuous quest to calibrate the nation's legal norms in alignment with the ever-evolving contours of the digital age. As the frontier of technological innovation pushes onward, the legal system's adaptive prowess will be vital in steering the course, orchestrating the symphony of innovation, justice, and societal well-being in harmony with the digital symphony.

References

Adams, R., & Adeleke, F. (2020). Protecting information rights in South Africa: the strategic oversight roles of the South African Human Rights Commission and the Information Regulator. *International Data Privacy Law*, *10*(2), 146–159. https://doi.org/10.1093/idpl/ipz022

Botha, J., Grobler, M., Hahn, J., & Eloff, M. (2017). A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws. In *The 12th International Conference on Cyber Warfare and Security (ICCWS)*. https://goo.su/e5JBlq

Bester, K. J. (2023). *Exploring the views and perceptions of cybersecurity among south african military officers*. https://goo.su/r7BU4

Bronstein, V. (2022). Prioritising Command-and-Control Over Collaborative Governance: The Role of the Information Regulator Under the Protection of Personal Information Act. *Potchefstroom Electronic Law Journal*, *25*, 1–41. https://doi.org/10.17159/1727-3781/2022/v25i0a11661

Burchell, J. (2009). 'The legal protection of privacy in South Africa: A transplantable hybrid'. *Electronic Journal of Comparative Law (EJCL)*, *13*(1) 1–26. https://clck.ru/36csJ3

de Bruyn, M. (2014). The Protection of Personal Information (POPI) Act – Impact on South Africa. *International Business & Economics Research Journal (IBER)*, *13*(6), 1315–1340. https://doi.org/10.19030/iber.v13i6.8922

De Sousa, W. G., Fidelis, R. A., De Souza Bermejo, P. H., Da Silva Gonçalo, A. G., & De Souza Melo, B. (2021). Artificial intelligence and speedy trial in the judiciary: Myth, reality or need? A case study in the Brazilian Supreme Court (STF). *Government Information Quarterly*, *39*(1), 101660. https://doi.org/10.1016/j.giq.2021.101660

Dove, E. S., & Chen, J. (2020). Should consent for data processing be privileged in health research? A comparative legal analysis. *International Data Privacy Law*, *10*(2), 117–131. https://doi.org/10.1093/idpl/ipz023

Kahungi, N. (2022). Dawn of Artificial Intelligence in Alternative Dispute Resolution; Expanding Access to Justice through Technology. *University of Nairobi Law Journal*, *2*(2). https://clck.ru/36csLM

Malgieri, G., & Comandé, G. (2017). Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. *International Data Privacy Law*, *7*(4), 243–265. https://doi.org/10.1093/idpl/ipx019

Mokofe, W. M., & van Eck, S. (2021). Reflections on Marginalised Workers and the Role of Trade Unions in the Changing World of Work. *Industrial Law Journal*, *41*(3), 1365–1389. https://clck.ru/36csMJ

Mokofe, W. M., & van Eck, S. (2022). COVID-19 at the workplace: What lessons are to be gained from early case law? *De Jure Law Journal*, *55*(1). https://doi.org/10.17159/2225-7160/2022/v55a10

Mtuze, S. (2022). The convergence of legislation on cybercrime and data protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 & the Protection of Personal Information Act 4 of 2013. *Obiter*, *43*(3), 536–569. https://doi.org/10.17159/obiter.v43i3.14883

Naude, A., & Papadopoulos, S. (2016). Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments. *Journal of Contemporary Roman-Dutch Law*, *79*, 51–68. https://clck.ru/36csPA

Roos, A. (2020). The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'. *Comparative and International Law Journal of Southern Africa*, *53*(3), 37. https://doi.org/10.25159/2522-3062/7985

Staunton, C., & De Stadler, E. (2019). Protection of Personal Information Act No. 4 of 2013: Implications for biobanks. *South Africa Medical Journal*, *109*(4), 232–234. https://doi.org/10.7196/samj.2019.v109i4.13617

Swales, L. (2018). An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One. *Potchefstroom Electronic Law Journal*, *21*, 1–30. https://doi.org/10.17159/1727-3781/2018/v21i0a2916

Swales, L. (2021). The Protection of Personal Information Act and data de-identification. *South African Journal of Science*, 117(7/8). https://doi.org/10.17159/sajs.2021/10808

Swales, L. (2022). The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock? *Potchefstroom Electronic Law Journal*, 25, 1–32. https://doi.org/10.17159/1727-3781/2022/v25i0a11180

Talkmore, C. (2022). The role of intellectual property rights' protection in advancing development in South Africa. *Law, Democracy and Development*, *26*,168189. https://doi.org/10.17159/2077-4907/2021/ldd.v26.7

Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. *The African Journal of Information and Communication (AJIC)*, *20*, 113–132. https://doi.org/10.23962/10539/23573

Van Niekerk, B. (2018). The Cybersecurity Dilemma: considerations for investigations in the Dark Web. *African Journal of Criminology & Victimology*, *31*(3), 132148. https://clck.ru/36csS9

Author information

William Manga Mokofe – PhD (Law), Advocate of the High Court of South Africa
Address: 12 Stewart Drive Berea, East London, South Africa
E-mail: william.mokofe@gmail.com
ORCID iD: https://orcid.org/0000-0002-5170-1304
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=h_w4XXAAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
ASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – August 22, 2023
Date of approval – October 11, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:341.492:343.11
EDN: https://elibrary.ru/dtiann
DOI: https://doi.org/10.21202/jdtl.2023.47

Цифровые преобразования южноафриканского правового ландшафта

Уильям Манга Мокофе

Верховный Суд Южно-Африканской Республики
г. Ист-Лондон, Южно-Африканская Республика

Ключевые слова

законодательство,
защита персональных данных,
искусственный интеллект,
киберпреступность,
онлайн-разрешение споров,
право интеллектуальной собственности,
право,
судебная практика,
цифровые технологии,
Южная Африка

Аннотация

Цель: Южная Африка является страной с большим потенциалом интенсивного развития благодаря стремительному росту и внедрению цифровых технологий. Активно формирующаяся цифровая среда трансформирует законодательную базу, которая в свою очередь оказывает влияние на цифровую среду. Это преобразующее взаимоотношение обусловило направленность исследования на выявление адаптивности правовой системы перед лицом динамичных изменений и путей эволюции правового ландшафта в условиях цифровизации и технологического прогресса.

Методы: изучение изменяющегося правового ландшафта требует междисциплинарного подхода, сочетающего юридический анализ с идеями из областей социологии, экономики и др. При этом с помощью формально-юридического метода исследуются ключевые правовые акты, формирующие цифровую среду Южной Африки и определяющие возможности и проблемы взаимодействия цифровых технологий и южноафриканского права.

Результаты: в работе дается представление о том, как правовая система Южной Африки решает цифровые проблемы; оценивается интеграция цифровых новаций в правовую систему; подчеркивается преобразующее влияние цифровых технологий на традиционные юридические процессы, охватывающие сбор доказательств, разрешение споров и доступ к правосудию; оценивается роль цифровых технологий в повышении эффективности юридических процессов.

Научная новизна: исследование вносит вклад в продолжающуюся дискуссию о сложной взаимосвязи между цифровыми технологиями и законодательством Южной Африки; показано, как южноафриканское

право справляется с цифровыми сложностями; обосновываются новые идеи о трансформации традиционной правовой парадигмы в результате цифровизации, ее последствий для судопроизводства и доступа к правосудию. При углублении в адаптацию, проблемы и инновации, возникающие на пересечении права, технологий и цифровизации, происходит понимание того, как южноафриканское право ориентируется в динамичной цифровой среде.

Практическая значимость: адаптация правового ландшафта к цифровизации и технологическим достижениям имеет решающее значение для обеспечения быстрого технологического прогресса и требует сотрудничества между государственными органами, гражданским обществом, экспертами в области права и технологий. Исследование содержит ценные рекомендации и предложения для политиков, юристов-практиков и заинтересованных сторон, формирующих правовую экосистему Южно-Африканской Республики, решающих проблемы обеспечения конфиденциальности персональных данных, повышения эффективности электронных взаимодействий и противодействия киберпреступности. Подчеркивается важность внедрения технологического прогресса при одновременном соблюдении надежных правовых гарантий.

Для цитирования

Мокофе, У. М. (2023). Цифровые преобразования южноафриканского правового ландшафта. *Journal of Digital Technologies and Law*, *1*(4), 1087–1104. https://doi.org/10.21202/jdtl.2023.47

Список литературы

Adams, R., & Adeleke, F. (2020). Protecting information rights in South Africa: the strategic oversight roles of the South African Human Rights Commission and the Information Regulator. *International Data Privacy Law*, *10*(2), 146–159. https://doi.org/10.1093/idpl/ipz022

Botha, J., Grobler, M., Hahn, J., & Eloff, M. (2017). A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws. In *The 12th International Conference on Cyber Warfare and Security (ICCWS)*. https://goo.su/e5JBlq

Bester, K. J. (2023). *Exploring the views and perceptions of cybersecurity among south african military officers*. https://goo.su/r7BU4

Bronstein, V. (2022). Prioritising Command-and-Control Over Collaborative Governance: The Role of the Information Regulator Under the Protection of Personal Information Act. *Potchefstroom Electronic Law Journal*, *25*, 1–41. https://doi.org/10.17159/1727-3781/2022/v25i0a11661

Burchell, J. (2009). 'The legal protection of privacy in South Africa: A transplantable hybrid'. *Electronic Journal of Comparative Law (EJCL)*, *13*(1) 1–26. https://clck.ru/36csJ3

de Bruyn, M. (2014). The Protection of Personal Information (POPI) Act – Impact on South Africa. *International Business & Economics Research Journal (IBER)*, *13*(6), 1315–1340. https://doi.org/10.19030/iber.v13i6.8922

De Sousa, W. G., Fidelis, R. A., De Souza Bermejo, P. H., Da Silva Gonçalo, A. G., & De Souza Melo, B. (2021). Artificial intelligence and speedy trial in the judiciary: Myth, reality or need? A case study in the Brazilian Supreme Court (STF). *Government Information Quarterly*, *39*(1), 101660. https://doi.org/10.1016/j.giq.2021.101660

Dove, E. S., & Chen, J. (2020). Should consent for data processing be privileged in health research? A comparative legal analysis. *International Data Privacy Law*, *10*(2), 117–131. https://doi.org/10.1093/idpl/ipz023

Kahungi, N. (2022). Dawn of Artificial Intelligence in Alternative Dispute Resolution; Expanding Access to Justice through Technology. *University of Nairobi Law Journal*, *2*(2). https://clck.ru/36csLM

Malgieri, G., & Comandé, G. (2017). Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. *International Data Privacy Law*, *7*(4), 243–265. https://doi.org/10.1093/idpl/ipx019

Mokofe, W. M., & van Eck, S. (2021). Reflections on Marginalised Workers and the Role of Trade Unions in the Changing World of Work. *Industrial Law Journal*, *41*(3), 1365–1389. https://clck.ru/36csMJ

Mokofe, W. M., & van Eck, S. (2022). COVID-19 at the workplace: What lessons are to be gained from early case law? *De Jure Law Journal*, *55*(1). https://doi.org/10.17159/2225-7160/2022/v55a10

Mtuze, S. (2022). The convergence of legislation on cybercrime and data protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 & the Protection of Personal Information Act 4 of 2013. *Obiter*, *43*(3), 536–569. https://doi.org/10.17159/obiter.v43i3.14883

Naude, A., & Papadopoulos, S. (2016). Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments. *Journal of Contemporary Roman-Dutch Law*, *79*, 51–68. https://clck.ru/36csPA

Roos, A. (2020). The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'. *Comparative and International Law Journal of Southern Africa*, *53*(3), 37. https://doi.org/10.25159/2522-3062/7985

Staunton, C., & De Stadler, E. (2019). Protection of Personal Information Act No. 4 of 2013: Implications for biobanks. *South Africa Medical Journal*, *109*(4), 232–234. https://doi.org/10.7196/samj.2019.v109i4.13617

Swales, L. (2018). An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One. *Potchefstroom Electronic Law Journal*, *21*, 1–30. https://doi.org/10.17159/1727-3781/2018/v21i0a2916

Swales, L. (2021). The Protection of Personal Information Act and data de-identification. *South African Journal of Science*, 117(7/8). https://doi.org/10.17159/sajs.2021/10808

Swales, L. (2022). The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock? *Potchefstroom Electronic Law Journal*, 25, 1–32. https://doi.org/10.17159/1727-3781/2022/v25i0a11180

Talkmore, C. (2022). The role of intellectual property rights' protection in advancing development in South Africa. *Law, Democracy and Development*, *26*,168189. https://doi.org/0.17159/2077-4907/2021/ldd.v26.7

Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. *The African Journal of Information and Communication (AJIC)*, *20*, 113–132. https://doi.org/10.23962/10539/23573

Van Niekerk, B. (2018). The Cybersecurity Dilemma: considerations for investigations in the Dark Web. *African Journal of Criminology & Victimology*, *31*(3), 132148. https://clck.ru/36csS9

Информация об авторе

Мокофе Уильям Манга, PhD в области права, адвокат Верховного Суда Южно-Африканской Республики
Адрес: Южно-Африканская Республика, г. Ист-Лондон, Стюарт Драйв Береа, 12
E-mail: william.mokofe@gmail.com
ORCID iD: https://orcid.org/0000-0002-5170-1304
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=h_w4XXAAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.91 / Государство и право отдельных стран
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 22 августа 2023 г.
Дата одобрения после рецензирования – 11 октября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.48

Effectiveness of the Administration of Justice in Nigeria Under the Development of Digital Technologies

Paul A. Aidonojie ✉

Edo State University Uzairue
Iyamho, Nigeria

Saminu A. Wakili

Edo State University Uzairue
Iyamho, Nigeria

David Ayuba

Edo State University Uzairue
Iyamho, Nigeria

Keywords

administration of justice,
court,
digital platform,
digital technologies,
electronic justice,
electronic record keeping,
law,
online court proceedings,
online dispute management,
virtualization of court proceedings

Abstract

Objective: the traditional Nigerian judicial system has long been associated with a conservative approach and traditional methodologies of justice administration. As a developing country, Nigeria has benefited immensely from the advancement of digital technology, especially in the legal field. This is due to the fact that modern digital technologies are being rapidly adopted in Nigeria's judicial processes for effective justice administration. However, despite the promise of digital technology, there are legal and socio-economic challenges in Nigeria that may affect its successful utilization in legal proceedings. This justifies the focus of the study – to identify the legal and socio-economic challenges of digitalization of court proceedings in Nigeria.

Methods: the study combines doctrinal and non-doctrinal approaches. The former ensures theoretical understanding of the conceptual issues

✉ Corresponding author

and prospects of court proceedings virtualization. It also allows exploring, based on primary and secondary sources (laws, monographs, research articles and internet resources), the legal and socio-economic challenges of the use of digital technologies in court proceedings. The non-doctrinal approach consists in polling, describing and analyzing the results of a sociological survey. The survey was conducted among Nigeria residents to reveal their attitudes towards innovations in digitalization and virtualization of court proceedings as well as the challenges posed by these processes.

Results: the study revealed that the use of digital technologies in court proceedings in Nigeria has several prospects of ensuring effective justice administration and accurate recording and storage of information. Along with the benefits, challenges are shown that may reduce the effectiveness of court proceedings digitalization.

Scientific novelty: consists in investigating the use of digital technology in Nigerian court proceedings and identifying the prospects of improving the efficiency of justice administration in Nigeria under digitalization, as well as the challenges arising from this trend.

Practical significance: the study will enable stakeholders in the Nigerian legal sector to identify legal and socio-economic challenges that may adversely affect and render ineffective the use of digital technologies in legal proceedings. In addition, the article offers practical recommendations to address these challenges.

For citation

Aidonojie, P. A., Wakili, S. A., & Ayuba, D. (2023). Effectiveness of the administration of justice in Nigeria under the development of digital technologies. *Journal of Digital Technologies and Law, 1*(4), 1105–1131. https://doi.org/10.21202/jdtl.2023.48

Contents

Introduction

Digital technology has become a significant tool in the legal profession that promotes and enhances the judicial system globally through efficiency, effective and quick access to the information for dispensation of justice (Meredith et al., 2021). In developed countries, advancements in technology have markedly refined and expedited judicial procedures (Machado et al., 2018). This is concerning the fact that most of these developed countries have a well enhanced and effective use of digital technology in the administration court proceedings. However, the traditional Nigerian judicial court system has long been associated with its conservative approach and conventional methodologies in the dispensation of justice (Olubukola & Abimbola, 2022). This situation over time has proved to be unfavourable to the judicial system in Nigeria coupled with the volume of cases before courts that needed to be decided on and other socio-economic challenges affecting the dispensation of justice (Olubukola & Abimbola, 2022). In this regard, it suffices to state that in light of the ever-evolving global technology, there exists a pressing necessity to enhance the efficiency and efficacy of Nigeria's court proceedings. Consequently, integrating virtual court proceedings into the judicial system of Nigeria has become imperative, offering a pathway to enhanced access to electronic case management and court sessions.

Concerning the above, to surmount the existing challenges of the Nigerian physical court proceedings, a directive was issued by the Attorney General of the Federation, Abubakar Malami, and the National Judicial Council, that courts should resort to digital virtual court proceedings (Olubukola & Abimbola, 2022). Flowing from the directives given, some states like Lagos, Abuja, and Rivers state resorted to remote court proceedings. For instance, Lagos State signed the Lagos State Judiciary Remote Hearing of Cases Practice Direction that came into effect on the 4th of May, 2020 (Mohamad & Sule, 2021). The purpose of making practice directions to accommodate digital virtual hearing is to hear cases that are not

urgent and time-bound via video or audio-conferencing platforms, such as Zoom, Skype, Google Meet or any of the platforms as may be approved by the court (Mohamad & Sule, 2021). Borno State was the first to use this medium where the judgment was delivered via online sitting in criminal matters, while other states are yet to witness this new development.

Though this new development is laudable and imperative in a world where technology is permeating all fields of endeavour (Granot et al., 2018; Goethe et al., 2021), especially in a situation that necessitated its emergence, its constitutionality has become a subject of contention in Nigeria (Tait & Tay, 2019). Some have argued that the extant provision of the Constitution which demands public trials though with some exceptions is not given full expression as stated under sections 36(1), (3), and (4) of the 1999 Constitution of the Federal Republic of Nigeria as amended. This category of persons has concluded that unless the Constitution is amended, the same cannot accommodate virtual court proceedings in Nigerian courts (Thornburg, 2021). The proponents of digital virtual court proceedings, on the other hand, have argued why the amendment of the Constitution is not necessary to give effect to virtual proceedings in Nigeria while proving its originality from the same Constitution (Winter et al., 2018).

It is concerning the above, that this study embarks on doctrinal and non-doctrinal examination of the prospect of digital virtual court proceedings in Nigerian courts. The study will also robustly discuss the legal issues surrounding digital virtual proceedings in Nigerian courts. The study will further discuss possible challenges to the use of technology in court sittings in Nigeria, and suggest some recommendations to salvage the identified challenges.

As for the research methodology, concerning the effective actualization of this study, a hybrid method of study (consisting of a doctrinal and non-doctrinal research method) was adopted. The essence of adopting the doctrinal method consists in enabling the researcher to theorize the conceptual issues and development of virtual court proceedings. Furthermore, it helps to examine the legal and socio-economic issues concerning digital virtual court proceedings. Hence, the study utilizes primary and reliable secondary sources such as laws, textbooks, articles in journals, and online articles.

Furthermore, the non-doctrinal method of research enabled the researchers to examine the respondents residing in Nigeria on the prospect and challenges of digital virtual court proceedings. In this regard, a questionnaire was generated through the use of Google form and distributed to a diverse audience. The data generated were analyzed using a descriptive and analytical method.

1. Conceptual Nature of Digital Virtual Court Proceedings in Nigeria

Various research endeavors have highlighted the confinement of Nigeria's judicial system within the traditional confines of courthouses (Mohamad & Sule, 2021; Bandes & Feigenson, 2021). These spaces include lawyers' chambers, reception areas, lounges, conference rooms, and law libraries brimming with printed resources (Bannon & Keith, 2021). Furthermore, areas designated for administrative assistants and paralegal offices are integral to the conventional

structure. Regrettably, this conventional approach has resulted in a surge of pending cases, protracted resolution processes, and a heightened challenge in accessing effective judicial services (Sanson et al., 2020). Furthermore, ensuring public access to judicial proceedings and safeguarding fundamental freedoms, as outlined in domestic legislation and international accords, has emerged as a pivotal concern within Nigeria's judicial milieu. In this regard, it suffices to state that though the Nigeria physical court proceedings have their merits, they are also fraught with challenges and these challenges are as follows:

1. Nigeria's vast geographical landscape poses challenges for individuals to physically access courtrooms, especially in rural and remote areas. This limits access to justice and disproportionately affects marginalized populations.

2. The Nigerian judicial system is burdened with a high volume of cases, leading to congestion in courts and significant delays in the administration of justice.

3. Attending physical court proceedings can be financially burdensome for many individuals, involving expenses related to transportation, accommodation, and time away from work.

4. Also, in some cases, the physical presence of parties involved in litigation can lead to security risks, intimidation, or coercion.

However, in developed countries, advancements in technology have markedly refined and expedited judicial procedures (Rossner, 2021). Conversely, given the challenges often encountered in physical court proceedings in Nigeria, the progress of legal service-related technology is gradually developing. Consequently, integrating virtual proceedings into the Nigerian judicial system has become imperative, offering a pathway to enhanced access to electronic case management and court sessions.

Concerning the above, the term "digital virtual court proceedings" as operated in Nigeria refers to court proceedings conducted online, wherein judges, legal representatives, court staff, witnesses, security personnel, and other involved parties attend the proceedings via digital platforms or communication tools like Zoom, Google meeting, Skype, and similar computer/internet devices (Nir & Musial, 2022). In this context, "digital virtual technology" denotes an artificial or computer-generated reality as opposed to a physical, absolute presence. Furthermore, "Zoom, Skype, and Google meeting" refers to a digital virtual or video conferencing session. Participants can join these meetings using webcams or phones (Derksen et al., 2020). A "Zoom, Skype, and Google meeting room" is the physical setup that enables individuals to initiate Zoom meetings, facilitating telecommuting and interaction (Legg & Song, 2021). Similarly, they are also a unified communications platform that integrates various business communication channels, such as online meetings, instant messaging, video conferencing, and more (Hwang et al., 2021).

In this regard, it suffices to state that digital virtual legal proceedings in Nigerian courts involve the utilization of digital platforms to conduct legal activities like hearings and trials

(Elek et al., 2012). This approach aims to improve accessibility, efficiency, and convenience by leveraging technology, allowing participants to engage in legal processes remotely (Bandes & Feigenson, 2020). This includes presenting evidence and making legal arguments without the need to be physically present in a physical courtroom (Bild et al., 2021). The implementation of virtual proceedings necessitates careful consideration of technological infrastructure and security measures, and ensuring that the legal processes remain fair and transparent (Bandes & Feigenson, 2020).

Furthermore, virtual court hearings can take two forms: hybrid or fully virtual (Fauville et al., 2021). In the hybrid approach, some parties are physically present in a specific location, while others participate online (Feigenson, 2010). This could involve scenarios where the judge, clerk, and witnesses are physically present in an open court, while other participants join virtually (Bunjavec, 2020). Alternatively, the judge, clerk, and lawyers might be present in open court, with witnesses joining remotely (Bailenson, 2021). On the other hand, the fully virtual method involves all parties participating from separate locations, including the judge, lawyers, witnesses, and clerks (Hans, 2022).

Concerning the above, it is apt to reiterate that the adoption of digital virtual court proceedings possesses several prospects which could enhance the practice of the Nigerian legal profession. In this regard, lawyers and those requesting justice must adapt to changing circumstances by adopting digital technology to enhance the administration of justice in Nigeria.

2. The Prospect of Digital Virtual Court Proceedings in Nigeria

The importance and prospects of virtual court proceedings in Nigeria can overcome the myriad of challenges of regular and physical convention court proceedings (Mohamad & Sule, 2021). The commencement of virtual court proceedings in Nigeria prompted extensive debates, with proponents and opponents expressing their viewpoints (Olubukola & Abimbola, 2022). These discussions underscored the advantages of implementing virtual court proceedings in Nigeria, while also addressing the challenges that must be resolved for the effective operation of such proceedings (Olubukola & Abimbola, 2022). Supporters of virtual court proceedings in Nigeria emphasized the convenience and prospect it tends to provide to the administration of justice in Nigeria's legal profession (Mohamad & Sule, 2021). Some of the prospects of digital virtual court proceedings as highlighted by these legal scholars are as follows:

- it is convenient;
- it saves unnecessary time wastage of traveling to physically attend court proceedings;
- it emphasizes the principles of fair hearing as stipulated in Nigeria's Constitution;
- it is cheaper and cost-effective;
- it rids of the challenge of distance which could serve as a barrier;
- it enables accurate records and storage of court proceedings;
- it reduces the workload of the judge and lawyers in taking record.

Flowing from the above it is with confidence in the face of shortcomings that may come with virtual proceedings to say that, it is a tool we embrace into the Nigerian court system fully, as this will enhance effective delivery and transparency in our judiciary and therefore restore the hope of the masses in our court system.

3. Legal Framework Concerning Virtual Proceedings in Nigeria Court

Concerning the legal framework of digital virtual proceedings in Nigeria Court, the statement Honourable Justice Kashim Zannah, Chief Judge of Borno State in his paper entitled "Advancements in Technology: Signpost or Requiem to Legal Practice" is very apt. According to him, the future of our legal market cannot be immune from the technology that will inevitably permeate the socio-economic fabrics of our society. His Lordship further argued that in the same way as dinosaurs went into extinction, paperwork in legal practice will follow suit.

Given this, the mixed reactions, and argument for and against the practice of virtual proceedings in Nigeria Court can be put to rest by a thorough examination of the provisions of the Nigerian law. This is concerning the fact that the most surfacing question since the inception of the adoption of digital virtual court proceedings, is hinge on the legality within the Nigerian legal ecosystem. This question stemmed from the belief of all time that you cannot put something on anything and expect it to stand. So some legal pundits do not welcome digital virtual court proceedings of any form, on the ground that Nigerian law does not support digital virtual proceedings thus any practice of this sort is unconstitutional and illegal. Those in this category, further opined that for the virtual hearing to be legal in the Nigerian court, the Nigerian Constitution must be amended to accommodate it. While to others it is a welcome development and it is to them constitutional and legal. They maintained that the Constitution need not be amended.

Concerning the above, it suffices to state that the legality of digital virtual court proceedings in Nigeria is recognized and provided for in the Nigerian constitutional, statutory and judicial authorities. It serves as the legal framework for digital virtual court proceedings and is therefore examined as follows.

3.1. The Nigeria Constitution Recognition of Digital Virtual Court Proceedings

The 1999 Constitution of the Federal Republic of Nigeria (As Amended) is Nigerian's number one law. It is the Supreme law of the land to which every other law traces its validity. This concerns the fact that section 1(3) of the Nigeria Constitution stipulates that any law that is inconsistent with the provisions of the Constitution will be declared null and void to the extent of such inconsistency. In this regard, the relevant section as it concerns digital virtual court proceedings is as provided for in Section 36(3) and (4). These provisions of the Constitution set a template as they relate to the validity of digital virtual court proceedings in Nigeria. Section 36(3) of the Nigerian Constitution provides that the proceedings of a court or any

tribunal shall be held in public. Furthermore, Section 36(4)(a) provides that a person charged before the court or tribunal shall be heard in public.

Concerning the above, it suffices to state that the combined reading of the above provisions of the Nigerian Constitution reveals that the major requirement for any proceedings to be valid or term court proceedings under the Nigerian Constitution is that such proceedings are held "in public". The emphasis is on the word "public". Furthermore, from the wordings of Sections 36(3) and (4), the contents of the subsections are a deliberate adventure that shows that it is mandatory for a court proceeding to be held in public. Once those requirements are met then such proceedings are qualified to be termed as Court proceedings. In confirming the legality of digital virtual court proceedings, it is very apt to state that the Nigerian Constitution never refers to a room, building, or place (as a physical location) to mean a court. By this, it is submitted that court is more of a service than a place accessible to the public. In this regard, it suffices to state that digital virtual court proceedings are open to the public, thus; court proceedings contemplated by the Nigerian Constitution. Though digital virtual court proceedings are not expressly mentioned by the Nigerian Constitution, but implied by the interpretation of Section 36(3) and (4) of the Nigerian Constitution. Commenting on the word "public" as used in Section 36 of the Nigerian Constitution, the court Per Muhammad JCA in Kosebinu & Ors v Alimi[1] opined that all that is required for a place to qualify as public as used under Section 36(3) of the 1999 Constitution of the Federal Republic of Nigeria is that the place should be accessible to the members of the public and not so accessible only on the permission or consent of the judge. Instructive in this regard, is the case of NAB Ltd v Barri Eng. Nig. Ltd, the Court, Per Belgore JSC posited that hearing in public entails a situation where the public is not barred.

Concerning the above, it suffices to state that though the Constitution does not expressly mention or provide for digital virtual court proceedings, but impliedly permits it, since a digital virtual platform can also be considered an even better public forum for court proceedings. Furthermore, it is a trite principle of law as judicially credited by the Nigerian Supreme Court in the case of Anyeabosi v. R.T Briscoe Ltd[2] that what is not prohibited is permitted. Also, the court held in Theophilus v FRN[3] that the basic principle or canon of statutory interpretation states that what is not expressly prohibited by statute is impliedly permitted. The court further stated that the court lacks interpretative jurisdiction or powers to interpret a statute to mean what it does not mean nor to interpret a law to not mean what it means. Furthermore, the Supreme Court, Per Obaseki JSC, in Attorney General of Bendel State v Attorney General of the Federation[4]; remarked and warned that the words

1 (2005) LPELR 11442 (CA).

2 (1987) 3 NWLR (Pt. 59) 108; Alhaji Ibrahim Hassan & Anor v Jafar Abubakar & Ors LER (2015) SC 732/2015.

3 (2012) LPELR 9846.

4 (1981) 10 SC 1.

of the Constitution should not be read with stuffing narrowness. For the sake of purposive interpretation of statutes therefore the court in FRN v Fani-Kayode[5] followed suit and restated the need for the court to adopt a proactive approach to the interpretation of law as well as the need for the court to avoid accepting disabilities not so imposed by law.

Thus, it is submitted in the light of the above authorities that the Nigerian Constitution does not prohibit digital virtual court proceedings in any of its provisions, and rather it impliedly permitted the use of digital technology in court proceedings. Furthermore, the Constitution in Section 36(3) (4) did not refer to any physical room or building so the word "court" is not restricted to a physical setting or building. In this regard, the meaning of the phrase "public hearing" as used in Section 36(3) and (4) of the Constitution is simply that it is accessible to the members of the public. Digital virtual court proceedings meet this requirement because it is accessible to the public; on this basis, it is arguable that digital virtual court proceedings in the Nigerian Court are legal and constitutional.

Furthermore, the legal framework on virtual proceedings in Nigeria Court can be stretched beyond the provisions of Section 36(3) and (4) of the Constitution and the judicial authorities. This is concerning the fact that by Sections 236, 248, 254, 259, 264, 269, 274, 279, and 284 of the Nigerian the Constitution of Nigeria, heads and Presidents of various courts are empowered to make rules known as the rules of Court for the practice and procedures to be observed in their respective courts as it seems best to them to achieve justice. In this regard, the provisions of Section 274 of the Constitution stipulate that the Chief Judge for each of the 36 Nigerian States is to make rules to regulate the practice and procedures of the High Court in their respective states. It was in keeping with this power and in exercising the same that some states in Nigeria have made rules that allow for digital virtual proceedings in their state.

Concerning this, there has been an arisen issue as to whether or not the practice direction made by the Chief Judges of these states on digital virtual court proceedings in their respective states is inconsistent with the provisions of Section 36(3) and (4) of the Nigerian Constitution, given the provisions of Section 274 of the Constitution among others that empower the Chief Judges of states to make rules for the regulations of practice and procedures in the State High Courts. The position of the law is that the Constitution is supreme and by Section 1(3) of the Nigeria Constitution any law that is found to be inconsistent with the provisions of the Constitution, the Constitution should prevail and such law should adjudge void to the extent to which it is inconsistent. In keeping with this, the court in Buhari v INEC[6] held that any practice direction that is found to be inconsistent with the provisions of Section 36(3) and 4 of the 1999 Constitution of the Federal Republic of Nigeria (As Amended) shall be null and void. But then, is the practice direction that makes for the practice of virtual proceedings in Nigeria Court inconsistent with the provisions of Section 36(3) and (4) of the Constitution

5 (2010) 14 NWLR (Pt.1214)481 at 503.

6 (2008) 3NWLR 465.

to make it qualify to suffer the fate of the consequence provided for under Section 1(3) of the Constitution and the authority in Buhari v INEC (Supra) thereby making it unconstitutional? In answering this question, the decision of the Supreme Court in the recent unreported case of Lagos State v Ekiti State Government[7] is instructive. In this case, the court had to determine whether having regard to the constitutional requirement that court proceedings, save for some exceptions, must be held in public and whether court hearings by the use of technology, by remote hearings of any kind, whether Zoom or WhatsApp, Microsoft Themes, Skype or any other audio-visual or video-conference platform are constitutional. The Supreme Court in resolving this issue described the matter as premature and speculative, dismissed the case and stated that by the current position of law in Nigeria digital virtual court proceedings are constitutional. This locus classicus case endorses digital virtual court proceedings in Nigerian Courts. This effort by the court was applauded by some legal luminaries including the former vice president of Nigeria, Prof. Yemi Osibanjo, SAN in a speech delivered at a webinar on Media Coverage of Virtual Court Proceedings in Nigeria. The learned Silk who described this decision as a welcoming development submitted in his speech that it has been years since the idea of computerization of court proceedings was considered, hence the endorsement of virtual court proceedings by a Supreme Court ruling is wise. He further stated that it has saved our system of justice from another catastrophic round of technical decisions around the constitutionality of digital virtual court proceedings among other issues.

Concerning the above, having established that virtual proceedings in Nigeria Court are legal and constitutional, it should be noted that apart from the Constitution and judicial authorities there are rules of the Court that provide for digital virtual court proceedings in Nigeria. The rules of the Court and practices directions that are of particular interest here are those of the National Industrial Court and the Lagos State High Courts.

3.2. The National Industrial Court of Nigeria Practice Directions and Guidelines, 2020

The National Industrial Practice Direction and Guidelines came into operation on the 18th of May 2020. The essence of the Practice Direction and Guidelines is aimed at ensuring access to speedy disposal of cases and justice. Furthermore, it was also aimed at seeking to keep with the lockdown directives that were meant to help control Coronavirus (Covid-19). However, it suffices to state that the Practice Direction sufficiently provides the procedure where court proceedings were done virtually through the use of electronic devices. This covers the entire court process from filing of processes to rulings. In this regard, Section 4(1) of the National Industrial Court of Nigeria Practice Directions and Guidelines for Court sitting provides for the filing of court processes electronically. It states that all documents that a party seeks to file must be scanned or converted to PDF format and sent

7 SC/CV/260/2020 (Unreported).

to the Court's registry through an electronic mail address or WhatsApp dedicated for that purpose. It further instructs that the counsel must sign and seal the process they seek to file. Subsection 2 of Section 4 of the Practice Direction, however, provides for physical means of filing where electronic filing becomes impracticable. Section 4(4) of Practice Direction provides that where a process is filed electronically, the parties and the counsel must drop an email or phone by which they can be reached. Section 5 of the Practice Direction, 2020 takes care of the payment of filing fees. Section 5(1) of the PD 2020 states that payment of filing fees should be electronically through remittal. Furthermore, Section 6 of the Practice Direction provides for the service of court processes as well as hearing notice/ electronic mode of service. Section 6(2), (3) and (4) provides that parties in all their process filed must indicate the contact address with email or phone number by which the court process is to be served on them both by the court officers and by the other party. This contact address is also required to notify the parties about the hearing notice. By Section 6(6) of the Practice Direction service is considered completed, delivered, and proper once the electronic device used for that service shows notice of delivery.

It suffices to state that the most relevant provision of the National Industrial Practice Direction and Guidelines is as provided for in Section 7(1). It stipulates that for digital virtual court proceedings as against physical hearings throughout the Covid-19 period except for extremely urgent and essential matters that may not be heard by the court virtually. The matter that falls under this category however is left for the Presidents of the National Industrial Court to list out and make them available for all judges to be guided. However, it is not all matters required to hold on digital virtual court proceedings, this is concerning the fact that Section 7(2) stipulates that all non-contentious matters or all cases that do not require evidence to be tendered or taken fall within the category of matters that can be heard remotely. It is also the purport of Subsection 2 that all judgments, rulings, and directions of the court are to be delivered virtually. Section 7(3) provides for the means or digital platform by which virtual court proceedings can be done. It expressly and specifically mentions video conferencing and further stipulates that any other means or digital technology platform that is approved by the court. It is apt to state that Section 7(7) of the Practice Direction and Guideline seems to re-emphasize the provisions of Sections 36(3) and (4) of the 1999 Nigerian Constitution. This is concerning the fact that this Section stipulates that the court must ensure that virtual hearing is accessible to the members of the public, except if it involves an exparte application or other proceedings required by any extant law or the rules of the Court to be conducted in chambers.

Concerning the above, it is apt to state that the practice direction and guidelines are by the provisions of Sections 36(3) and (4) of the Nigerian Constitution. Furthermore, it suffices to state the National Industrial Court Practice Directions and Guidelines 2020 seem to have provided for digital virtual court proceedings, though the practice direction and guidelines can only be enforced within National Industrial Court in Nigeria. In this regard, all other courts are not legally obligated to observe and implement the practice direction and guidelines.

3.3. Practice Direction for Remote Hearing of Cases in the Lagos Judiciary 2029

This practice direction was made and issued by the Chief Judge of Lagos State, Honourable Justice Kazeem O. Alogba. It should be stated this practice direction is made according to the provision of the Nigerian Constitution, the Administration of Criminal Justice Law, Lagos State, and Lagos State Rules of Court that empowers the Chief Judge to enact the practice direction and guidelines regulating court within the Lagos State jurisdiction. Section 5 of the Practice Direction, it is provided that all digital virtual court proceedings must adhere to the provisions of the Nigerian Constitution and all other applicable laws.

Sections 6–10 cover the filing of court processes, payment of filing process, and the service of Court process. In this regard, Section 7 of the practice direction stipulates that a document that is to be filed electronically must be scanned or converted to PDF format and conveyed to the Court registry via an email or WhatsApp consigned for that purpose. However, the proviso to Section 7 of the practice direction stipulates that where electronically filing becomes impracticable it can be filed physically at the court registry. Section 11 of the PD provides that service of court processes should be done electronically by email, WhatsApp, or by directives of the court if there are any. In this regard, Section 13 further stipulates that where service is considered electronically, the time begins to count from when it was sent and not when it was received.

The most relevant provisions of the practice directions and guidelines are Sections 14–18. These sections deal with the nature of digital virtual court proceedings, the platform to be used, and other modalities. In this regard, Section 14 stipulates that parties and counsel should meet and plan the virtual meeting with the registry. However, Section 16 of the practice direction and guidelines provide for the digital technology platform where virtual court proceedings can be held. They are: through Zoom, Skype, or any other communication method approved by the judge. Section 17 on the other hand directs that the parties and Counsel must ensure that the facilities needed for the digital virtual hearing are available. Furthermore, the section also stipulates that the notice of court hearing should be made available on the website of the judge and also be stated on the cause list. Furthermore, Section 19 of the practice direction stipulates that the court has to direct and instructs the parties and counsel on the use of video conferencing and audio during proceedings. Section 20 of the practice direction also made it compulsory that counsel appearing virtually must be appropriately dressed by the dress code of the legal profession. Concerning the recording of the digital virtual court proceeding, Section 21 empowers the court to record the court proceedings. However, Section 22 further stipulates that a counsel of parties can only record upon obtaining the leave of court.

Concerning the above provision of the Lagos State Practice Direction and Guidelines, it suffices to state that it substantially provides for virtual proceedings and is in conformity with Sections 36(3) and (4) of the Nigeria Constitution. In this regard, it will be apt to state that given the constitutional provision, statutory and judicial authority, digital virtual court proceedings are legal, constitutional, and permissible in the Nigerian Court system.

4. Legal and Socio-economic Challenges Concerning Digital Virtual Court Proceedings in Nigeria

It is apt to state that the introduction of virtual proceedings in Nigeria is a very welcoming development and is celebrated by many for its multiple benefits. However, it should be noted that this practice faces a lot of legal and socio-economic challenges in Nigeria. These challenges and the attendant issues are worth considering their amelioration so as to enjoy the smooth practice of virtual proceedings in Nigeria.

4.1. The issue of the constitutionality of virtual court proceedings in Nigeria

One major issue that followed the practice of virtual hearing is the question of constitutionality. This question is concerning the fact that there is an express mention of digital virtual court proceedings in Section 36 of the Nigeria Constitution. This is concerning the fact that Section 36(3) and (4) of the Constitution provides that the hearings by courts and tribunals must be held in public. It is in the interpretation of this subsection that a lot of issues arose. Lawyers, writers, professors of law, legal luminaries and probably even judges have divided opinions on this. While some legal scholars believe that digital virtual court proceedings are in breach of the constitutional requirement which hinges on the public hearing because the members of the public will not readily participate in the virtual court hearing. They further argued that given the requirements of the Constitution, the courts must ensure public access except in those very limited instances where public safety or public health is required. According to these scholars, digital virtual court proceedings tend to limit public participation in court proceedings, given the fact that not everyone could afford it. In this regard, they consider the practice direction and guidelines of most courts that permit and allow for digital virtual court proceedings as inconsistent with the Nigerian Constitution. However, it suffices to state that, this argument has been laid to rest by the decision of the Supreme Court in the case of Lagos State v Ekiti State Government (Supra) where the issue of the constitutionality of the virtual hearing was in issue. The Attorney General of Lagos and the Attorney General of Ekiti State approached the Supreme Court with their issues. The Court ruled to the surprise of many, yet rightly that virtual court proceedings are not unconstitutional in Nigeria and that it is by the provision of the Nigerian Constitution.

4.2. The challenges of Evidentiary Issues

The subject of evidence is very important in any court proceedings. Evidence is the wheel upon which judicial proceedings ride. Cases are lost and are won on the availability or otherwise of the evidence. It is a trite law that witnesses are often called to test the evidence tendered in court. These witnesses must pass through the heat of cross-examination. While it cannot be said that this is not entirely denied in digital virtual court proceedings, its efficacy and potency

are drastically reduced and affected. Furthermore, digital virtual court proceedings also pose a challenge and issue to the court in evaluating the credibility of a witness. Also, video quality and technological failures can interfere with the court's perception of a witness's evidence. Additionally, there is manifestly the need to bring the process of tendering evidence as well as its admissibility with the practice in the traditional court system. This is concerning the fact that Sections 86 and 90 of The Evidence Act; it stipulates that evidences are required to be tendered in physical form. This implies that evidence in soft copy forms is not recognized or tender through digital platforms is admissible. There is also the discovery that a document that has been tampered with can be tendered and admitted in evidence virtually without notice. This is because the shared screen feature may not be promising enough to expose any alteration or mutilation to a document that has been tampered with. Given the lack of a defined path and directive as to how evidence is to be tendered in digital virtual court proceedings, will therefore pose legal challenges.

4.3. Enforcement of Orders

Unlike what we are used to physically, enforcing court orders, such as serving documents or ensuring compliance with judgments, could become more challenging when it comes to digital virtual court proceedings. This challenge is perpetuated by the generality of issues that bedevil the digital technology environment.

4.4. Digital Literacy and Technophobia

Digital virtual court proceedings depend largely on the robust use of digital technology. Computer and digital literacy are necessary for the parties and especially counsel to navigate through this practice. This already has disadvantaged a lot of people who are not computer literate. This includes adults who will invariably display fear of technology instead of welcoming, accepting, and using it. Furthermore, it suffices to state that older judges and legal practitioners, who throughout their lives depended on paperwork and physical appearance in court, will be disadvantaged in using digital technology in court proceedings.

4.5. Infrastructural Issues

The importance of infrastructural build-up for the smooth and effective practice of digital virtual court proceedings cannot be overemphasized. To conduct virtual proceedings smoothly, there must be stable and uninterrupted internet connectivity, electric power supply, and access to electronic devices. But it suffices to say that, this is a major challenge that faces the Nigerian system of operation of digital technology. Most places in Nigeria do not have a constant power supply, and the network has also been a major issue that interrupts online or virtual meetings, virtual proceedings are not in any way immune from these challenges.

5. Presentation and Analysis of Data

The data generated through the use of an online questionnaire distributed to the respondents is therefore presented and examined as follows.

5.1. Sample Size and Techniques

To achieve a wider and sufficient wider scope of response from the respondents in Nigeria through the use of a questionnaire, the study was conducted among the respondents residing in Nigeria. The study's sample focused on a sample size of 303 respondents residing in Nigeria's various geo-political zones. However, in identifying or selecting the respondents to respond to the questionnaire, the study utilizes a simple random sampling method. The simple random method of sampling has been adjudged to have the following advantages and relevance:

– the random sampling method is more apt in identifying audiences or respondents from heterogenous populaces or inhabitants;

– the result generated by using the simple random sampling method is free from prejudice, unbiased, and dispassionate;

– using the random sampling method to identify respondents is less demanding and devoid of complications;

– it is considered relevant and advantageous in a hybrid legal research method.

5.2. Data Analysis

The data obtained or generated from the questionnaire are therefore presented in tables 1–6 for accuracy and clarity of presentation.

Table 1 shows valid respondents' identification of the various geo-political zones they reside or live in Nigeria.

Table 1. Valid respondents' identification of their residential area in Nigeria (303 responses)

S/N	Geopolitical Zones in Nigeria	Responses of Respondents	Percent
1	North Central	35	11.6
2	North East	37	12.2
3	North West	29	9.6
4	South East	67	22.1
5	South South	79	26.1
6	South West	56	18.5
	TOTAL	303	100

Table 2 shows clarifications and valid confirmation of the prospect digital virtual court proceedings tend to provide in the administration of justice in Nigeria.

Table 2. Valid respondents' confirmation of if there are prospects in adopting digital virtual court proceedings in Nigeria (303 responses)

	Response	Percent
Valid Yes	260	85.8
Valid No	43	14.2
Total	303	100

Table 3 shows clusters of identification of the prospects and relevance of digital virtual court proceedings in the administration of justice in Nigeria.

Table 3. Valid Cluster of identification of the prospects of digital virtual court proceedings (263 responses, more than one option could be chosen)

The prospect of digital virtual court proceedings	Cluster of Response	Percentage
It is convenient	157	59.7
It saves unnecessary time wastage of traveling in physically attending court proceedings	214	81.4
It emphasizes the principles of fair hearing as stipulated in Nigeria's constitution	194	73.8
It is cheaper and cost-effective	106	40.3
It rids of the challenge of distance which could serve as a barrier	210	79.8
It enables accurate records and storage of court proceedings	131	49.8
It reduces the workload of the judge and lawyers in taking record	185	70.3

Table 4 shows valid confirmations by respondents in identifying if there are challenges concerning the adoption and use of digital virtual court proceedings in Nigeria.

Table 4. Valid confirmation of if there are challenges to adopting digital virtual court proceedings in Nigeria (303 responses)

	Response	Percent
Valid Yes	259	85.5
Valid No	44	14.5
Total	303	100

Table 5 shows clusters of identification of challenges that may affect the effective use of digital virtual court proceedings in Nigeria.

Table 5. Cluster of challenges of digital virtual court proceedings in Nigeria (263 responses, more than one option could be chosen)

Challenges of digital virtual court proceedings	Cluster of Response	Percentage
Insufficient legal regulation of the use of digital virtual court proceedings	210	79.8
Its sophisticated nature could lead to permanent loss of information	201	76.4
Internet fraudsters could hack into the digital platform	149	56.7
Challenges of corruption by court officials in the manipulation of the processes	200	76
Poor and effective network	152	57.8
Epileptic power supply	141	53.6
Illiteracy and inability to operate digital virtual software by most lawyers and litigant	191	72.6

Table 6 shows valid responses of respondents in identifying possible ways in enhancing the use of digital virtual court proceedings in Nigeria.

Table 6. Valid cluster of remedies to enhance the use of digital virtual court proceedings in Nigeria (263 responses, more than one option could be chosen)

Strategy for enhancing digital virtual court proceedings	Cluster of Responses	Percentage
Review of the rules and laws of the court to adequately provide for digital virtual court proceedings	213	81
Provision of additional backup in court proceedings storage and record keeping	216	82.1
Strict prosecution of individuals involved in digital fraud	141	53.6
Sensitization and training of legal practitioners on the usage of digital virtual court proceedings	190	72.2
Enhancing the provision of an effective and stable network by network providers	161	61.2
Stable power supply	129	49

5.3. Discussion of Findings

Concerning the result of data that was generated in this study by the use of a questionnaire as presented and analyzed in the tabular format above, is therefore discussed as follows. In Table 1, 303 respondents were the sample size of the study that responded to the questionnaire and they are Nigerians who reside within the various parts of Nigeria. The essence of this is to ensure that the respondents possess the knowledge and are well-informed concerning the prospects and challenges of digital virtual court proceedings in Nigeria. Furthermore, in Table 2, 85.8 % of the respondents confirm that the adoption of digital virtual court proceedings seems to have several prospects in enhancing the administration of justice in Nigeria. In this regard, in Table 3, the respondents were able to identify some of the prospects, relevance, and advantages of digital virtual court proceedings as follows:

1. 59.7 and 81.4 % of the respondents stated that it is convenient and it saves unnecessary time wastage of traveling in physically attending court proceedings, respectively.

2. 73.8 % agreed that it emphasizes the principles of fair hearing as stipulated in Nigeria's Constitution.

3. 40.3 and 79.8 %, respectively, also stipulated that it is cheaper and cost-effective and rids of the challenge of distance which could serve as a barrier.

4. 49.8 % identify that it enables accurate records and storage of court proceedings.

5. Furthermore, 70.3 % of the respondents were of the view that it reduces the workload of the judge and lawyers in taking record.

Despite the beautiful and cogent prospect digital technology tends to provide, however, in Table 4, 85.5 % of the respondents representing the majority of the respondents confirm that there are challenges in adopting and using digital virtual court proceedings in Nigeria. In this regard, in Table 5, the respondents identify some of these challenges as follows; 79.8 %

of the respondents stated that there is insufficient legal regulation of the use of digital virtual court proceedings. 76.4 % of the respondents were of the opinion that the sophisticated nature of digital virtual court proceedings could lead to permanent loss of information. These findings showed the sophisticated nature of digital technology and poor method of operation, it could lead to loss of information and give room for internet fraudsters to intercept the smooth usage of digital platforms. 56.7 % identify that internet fraudsters could hack into the digital platform. 76 % stated that there are also the challenges of corruption by court officials in the manipulation of the processes. 57.8 and 53.6 % agreed that poor network and epileptic power supply respectively could be a major challenge. These findings also state that Nigeria is a developing country that has been unable to resolve issues of poor internet connection and electrical power supply. These have always posed challenges in the usage of digital technology in Nigeria. Furthermore, 72.6 % of the respondents stated that there is also a challenge of illiteracy and inability to operate digital virtual software by most lawyers and litigants.

However, despite the above challenges of digital virtual court proceedings in Nigeria, it suffices to state that the advantages and prospects are numerous. Furthermore, the global environment is transcending into a global digitalize village and Nigerians cannot afford to be left behind in crude methods of living. In this regard, in Table 6, the respondents suggested probable solutions to correcting the above legal and socio-economic challenges in adopting digital virtual court proceedings in Nigeria as follows:

1. 81 % of the respondents identify that there is a need for a review of the rules and laws of a court to adequately provide for digital virtual court proceedings.

2. 82.1 % stated that there should be the provision of additional backup in court proceedings storage and record keeping.

3. 53.6 % identify strict prosecution of individuals involved in digital fraud as a measure to enhance the use of digital virtual court proceedings in Nigeria.

4. Also, 72.2 % were of the opinion that there is a need for sensitization and training of legal practitioners on the usage of digital virtual court proceedings.

5. Furthermore, 61.2 % stated that there is a need in enhancing the provision of an effective and stable internet connection by network providers and stable power supply respectively.

Conclusion

The study has been able to examine the viability and prospect of digital virtual court proceedings in Nigeria. Furthermore, the study also identifies the fact that the Nigeria Constitution though does not expressly provide for and regulate digital virtual court proceedings, however, a careful examination of Section 36(3) and (4) of the Nigerian Constitution reveals that there is an implied approval and recognition of digital virtual court proceedings. Furthermore, the study further observed that this position of the law has been

judicially affirmed by the apex court in Nigeria. In furtherance of the constitutional power of the head of various courts in Nigeria to make rules concerning the operation of their court, the head of Lagos State High Court and National Industrial Court has through this medium enacted their practice direction and incorporated the adoption and regulation of digital virtual court proceedings.

However, it suffices to state that while digital virtual court proceedings offer the potential for increased efficiency and accessibility in the Nigerian court system, there are some legal and socio-economic challenges identified in this study that may affect its viability. In this regard, several critical considerations and recommendations should be taken into account as follows:

1. In keeping with the right to privacy guaranteed under Chapter 4 of the 1999 Constitution of the Federal Republic of Nigeria, the court should make very strong security measures to protect sensitive information, prevent unauthorized access, and maintain the confidentiality of court proceedings.

2. The court should improve on the current practice Direction and Guidelines so that there are guidelines and standards for managing technical glitches and conducting virtual proceedings, especially rules for presenting and tendering evidence.

3. The government and persons concerned should commit to investing in robust and reliable internet connectivity as well as power supply across the country to ensure seamless virtual proceedings without disruptions.

4. The Nigerian government and judiciary should from time to time organize training programs for lawyers, judges, and court staff to enhance their digital literacy skills, enabling them to effectively use virtual proceedings platforms and tools.

5. The court conducting virtual hearings should improve on making its proceeding accessible to all parties, including those with limited resources, by dropping the link in a designated place that is open to the public and also by providing necessary technology and support to bridge the digital divide.

6. The court should make a deliberate effort to make procedures for remote swearing of oaths to ensure the integrity of witness testimony as it is a common practice in traditional court.

References

Bailenson, J. N. (2021). Nonverbal overload: A theoretical argument for the causes of Zoom fatigue. *Technology, Mind, and Behavior*, *2*(1), 1–6. https://doi.org/10.1037/tmb0000030

Bandes, S. A., & Feigenson, N. (2020). Virtual trials: Necessity, invention, and the evolution of the courtroom. *Buffalo Law Review*, *68*(5), 1275–1352. https://doi.org/10.2139/ssrn.3683408

Bandes S. A., & Feigenson, N. (2021). Empathy and remote legal proceedings. *Southwestern Law Review*, *51*(1), 20–39. https://clck.ru/36dpJt

Bannon, A., & Keith, D. (2021). Remote Court: Principles for Virtual Proceedings during the Covid-19 Pandemic and Beyond. *Northwestern University Law Review*, *115*(6), 1875–1897. https://clck.ru/36ct2V

Bild, E., Redman, A., Newman, E. J., Muir, B. R., Tait, D., & Schwarz, N. (2021). Sound and credibility in the virtual court: Low audio quality leads to less favorable evaluations of witnesses and lower weighting of evidence. *Law and Human Behavior*, *45*(5), 481–495. https://doi.org/10.1037/lhb0000466

Bunjavec, T. (2020). *Judicial Self-Governance in the new Millennium – an Institutional and Policy Framework*.

Springer. https://doi.org/10.1007/978-981-33-6506-3

Derksen, D. G., Giroux, M. E., Connolly, D. A., Newman, E. J., & Bernstein, D. M. (2020). Truthiness and law: Nonprobative photos bias perceived credibility in forensic contexts. *Applied Cognitive Psychology*, *34*(6), 1335–1344. https://doi.org/10.1002/acp.3709

Elek, J. K., Ware, L. J., & Ratcliff, J. J. (2012). Knowing when the camera lies: Judicial instructions mitigate the camera perspective bias. *Legal and Criminological Psychology*, *17*(1), 123–135. https://doi.org/10.1111/j.2044-8333.2010.02000.x

Fauville, G., Luo, M., Queiroz, A. C. M., Bailenson, J. N., & Hancock, J. (2021). Nonverbal mechanisms predict Zoom fatigue and explain why women experience higher levels than men. *SSRN Electronic Journal*, 1–18. https://doi.org/10.2139/ssrn.3820035

Feigenson, N. (2010). Visual evidence. *Psychonomic Bulletin & Review*, *17*(2), 149–154. https://doi.org/10.3758/PBR.17.2.149

Goethe, O., Sørum, H., & Johansen, J. (2021). The effect or non-effect of virtual versus non-virtual backgrounds in digital learning. In T. Ahram, & R. Taiar (Eds.), *Lecture notes in networks and systems: Vol. 319. Human interaction, emerging technologies and future systems* (pp. 274–281). Springer. https://doi.org/10.1007/978-3-030-85540-6_35

Granot, Y., Feigenson, N., Balcetis, E., & Tyler, T. (2018). In the eyes of the law: Perception versus reality in appraisals of video evidence. *Psychology, Public Policy, and Law*, *24*(1), 93–104. https://doi.org/10.1037/law0000137

Hans, V. P. (2022). Virtual juries. *DePaul Law Review*, *71*(2), 301–330. http://dx.doi.org/10.2139/ssrn.3860165

Hwang, A. H.-C., Wang, C. Y., Yang, Y.-Y., & Won, A. S. (2021). Hide and seek: Choices of virtual backgrounds in video chats and their effects on perception. In *Proceedings of the ACM on Human-Computer Interaction* (Vol. 5, Iss. CSCW2, pp. 1–22). New York, NY. https://doi.org/10.1145/3476044

Legg, M., & Song, A. (2021). The courts, the remote hearing and the pandemic: From action to reflection. *University of New South Wales Law Journal*, *44*(1), 126–166. https://doi.org/10.53637/ZATE4122

Machado, M., Sousa, M., Rocha, V. & Isidro, A. (2018). Innovation in judicial services: a study of innovation models in labor courts. *Innovation & Management Review*, *15*(2), 155–173. https://doi.org/10.1108/INMR-04-2018-010

Meredith, R., David, T., & McCurdy, M. (2021). Justice reimagined: challenges and opportunities with implementing virtual courts. *Current Issues in Criminal Justice*, *33*(4), 1–17. https://doi.org/10.1080/10345329.2020.1859968

Mohamad, A. M., & Sule, I. (2021). ICT-Enabled Applications for Decision-Making by the Courts: Experiences from Malaysia and Nigeria. *International Journal of Law, Government and Communication*, *6*(22), 189–196. https://doi.org/10.35631//ijlgc.6220018

Nir, E., & Musial, J. (2022). Zooming in: Courtrooms and defendants' rights during the COVID-19 pandemic. *Social & Legal Studies*, *31*(5), 725–745. https://doi.org/10.1177/09646639221076099

Olubukola, O., & Abimbola, D. (2022). Remote Court Proceedings in Nigeria: Justice Online or Justice on the Line. *International Journal for Court Administration*, *13*(2), 21–38. https://doi.org/10.36745/ijca.448

Rossner, M. (2021). Remote rituals in virtual courts. *Journal of Law and Society*, *48*(3), 334–361. https://doi.org/10.1111/jols.12304

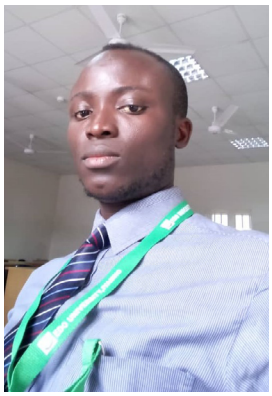
Sanson, M., Crozier, W. E., & Strange, D. (2020). Court case context and fluency-promoting photos inflate the credibility of forensic science. *Zeitschrift für Psychologie*, *228*(3), 221–225. https://doi.org/10.1027/2151-2604/a000415

Tait, D., & Tay, V. (2019). *Virtual court study: Report of a pilot test 2018*. Western Sydney University. https://doi.org/10.26183/5d01d1418d757

Thornburg, E. G. (2021). Observing online courts: Lessons from the pandemic. *SSRN Electronic Journal*, *54*(3), 181–244. https://doi.org/10.2139/ssrn.3696594

Winter, B., Daguna, J., & Matlock, T. (2018). Metaphor-enriched social cognition and spatial bias in the courtroom. *Metaphor and the Social World*, *8*(1), 81–99. https://doi.org/10.1075/msw.17001.win

Authors information



Paul Atagamen Aidonojie – PhD, Lecturer, Edo State University Uzairue
Address: 689M+PP5, 312107, Auchi/Abuja Express Way, Iyamho, Edo State, Nigeria
E-mail: aidonojie.paul@edouniversity.edu.ng
ORCID ID: https://orcid.org/0000-0001-6144-2580
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57221636261
Google Scholar ID: https://scholar.google.com/citations?user=0h9E2ZIAAAAJ

Saminu Abacha Wakili – Assistant Researcher, Edo State University Uzairue
Address: 689M+PP5, 312107, Auchi/Abuja Express Way, Iyamho, Edo State, Nigeria
E-mail: wakili18.saminu@edouniversity.edu.ng
ORCID ID: https://orcid.org/0009-0000-7043-286X

David Ayuba – Assistant Researcher, Faculty of Law, Edo State University Uzairue
Address: 689M+PP5, 312107, Auchi/Abuja Express Way, Iyamho, Edo State, Nigeria
E-mail: ayuba18.david@edouniversity.edu.ng
ORCID ID: https://orcid.org/0009-0008-7706-9627

Authors' contributions

Paul Atagamen Aidonojie provided overall guidance and set the study objectives; searched and selected the scientific literature; critically evaluated the interpretation of the study results; formulated the key findings, suggestions and recommendations; and approved the final version of the article.
Saminu Abacha Wakili analyzed the national legislation; interpreted the study findings; organized the sociological survey; and drafted the manuscript.
David Ayuba collected and analyzed literature and legislation; conducted the sociological survey; interpreted the study results; and prepared the manuscript.

Conflict of interest

The authors declare no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – August 18, 2023
Date of approval – October 25, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:341.492:343.11
EDN: https://elibrary.ru/zxufeq
DOI: https://doi.org/10.21202/jdtl.2023.48

Эффективность отправления правосудия в Нигерии в условиях развития цифровых технологий

Пол А. Айдоноджи ✉

Государственный университет Эдо-Узайруэ
г. Иямхо, Нигерия

Самину А. Вакили

Государственный университет Эдо-Узайруэ
г. Иямхо, Нигерия

Давид Аюба

Государственный университет Эдо-Узайруэ
г. Иямхо, Нигерия

Ключевые слова

виртуализация судопроизводства,
онлайн-разрешение споров,
онлайн-судопроизводство,
отправление правосудия,
право,
суд,
цифровая платформа,
цифровые технологии,
электронное делопроизводство,
электронное правосудие

Аннотация

Цель: традиционная нигерийская судебная система долгое время ассоциировалась с ее консервативным подходом и традиционными методологиями отправления правосудия. В результате развития цифровых технологий Нигерия как развивающаяся страна получила огромные преимущества, особенно в правовой сфере. Это связано с тем, что для эффективного отправления правосудия в судопроизводство Нигерии стремительно внедряются современные цифровые технологии. Однако, несмотря на перспективы развития цифровых технологий, в Нигерии существуют правовые и социально-экономические проблемы, которые могут повлиять на успешное их использование в судопроизводстве. Этим обосновывается нацеленность исследования на выявление правовых и социально-экономических проблем цифровизации судопроизводства в Нигерии.

Методы: исследование сочетает в себе доктринальный и недоктринальный подходы. Первый позволяет теоретически осмыслить концептуальные вопросы и перспективы развития виртуализации

✉ Контактное лицо

судопроизводства, изучить на основе первичных и вторичных источников (законов, монографий, научных статей и интернет-ресурсов) правовые и социально-экономические проблемы использования цифровых технологий в судопроизводстве. Второй направлен на анкетирование, описание и анализ результатов социологического опроса, проведенного среди респондентов, проживающих в Нигерии, на предмет их отношения к нововведениям в области цифровизации и виртуализации судопроизводства, а также к возникающим в связи с цифровизацией проблемам.

Результаты: исследование показало, что использование цифровых технологий в судопроизводстве Нигерии имеет ряд перспектив, обеспечивающих эффективное отправление правосудия и обеспечение точного учета и хранения данных о судебных заседаниях. Наряду с преимуществами показаны проблемы, которые могут повлиять на эффективность цифровизации судопроизводства.

Научная новизна: заключается в исследовании использования цифровых технологий в судопроизводстве Нигерии, в выявлении перспективы повышения эффективности отправления нигерийского правосудия в условиях развития цифровых технологий, а также в обусловленных этой тенденцией проблем.

Практическая значимость: исследование позволит заинтересованным сторонам нигерийского юридического сектора выявить правовые и социально-экономические проблемы, которые могут негативно повлиять на использование цифровых технологий в судопроизводстве и сделать их неэффективными. Кроме того, в статье предлагаются конкретные (практические) рекомендации по устранению этих проблем.

Для цитирования

Айдоноджи, П. А., Вакили, С. А., Аюба, Д. (2023). Эффективность отправления правосудия в Нигерии в условиях развития цифровых технологий. *Journal of Digital Technologies and Law*, *1*(4), 1105–1131. https://doi.org/10.21202/jdtl.2023.48

Список литературы

Bailenson, J. N. (2021). Nonverbal overload: A theoretical argument for the causes of Zoom fatigue. *Technology, Mind, and Behavior*, *2*(1), 1–6. https://doi.org/10.1037/tmb0000030

Bandes, S. A., & Feigenson, N. (2020). Virtual trials: Necessity, invention, and the evolution of the courtroom. *Buffalo Law Review*, *68*(5), 1275–1352. https://doi.org/10.2139/ssrn.3683408

Bandes S. A., & Feigenson, N. (2021). Empathy and remote legal proceedings. *Southwestern Law Review*, *51*(1), 20–39. https://clck.ru/36dpJt

Bannon, A., & Keith, D. (2021). Remote Court: Principles for Virtual Proceedings during the Covid-19 Pandemic and Beyond. *Northwestern University Law Review*, *115*(6), 1875–1897. https://clck.ru/36ct2V

Bild, E., Redman, A., Newman, E. J., Muir, B. R., Tait, D., & Schwarz, N. (2021). Sound and credibility in the virtual court: Low audio quality leads to less favorable evaluations of witnesses and lower weighting of evidence. *Law and Human Behavior*, *45*(5), 481–495. https://doi.org/10.1037/lhb0000466

Bunjavec, T. (2020). *Judicial Self-Governance in the new Millennium – an Institutional and Policy Framework*. Springer. https://doi.org/10.1007/978-981-33-6506-3

Derksen, D. G., Giroux, M. E., Connolly, D. A., Newman, E. J., & Bernstein, D. M. (2020). Truthiness and law: Nonprobative photos bias perceived credibility in forensic contexts. *Applied Cognitive Psychology*, *34*(6), 1335–1344. https://doi.org/10.1002/acp.3709

Elek, J. K., Ware, L. J., & Ratcliff, J. J. (2012). Knowing when the camera lies: Judicial instructions mitigate the camera perspective bias. *Legal and Criminological Psychology*, *17*(1), 123–135. https://doi.org/10.1111/j.2044-8333.2010.02000.x

Fauville, G., Luo, M., Queiroz, A. C. M., Bailenson, J. N., & Hancock, J. (2021). Nonverbal mechanisms predict Zoom fatigue and explain why women experience higher levels than men. *SSRN Electronic Journal*, 1–18. https://doi.org/10.2139/ssrn.3820035

Feigenson, N. (2010). Visual evidence. *Psychonomic Bulletin & Review*, *17*(2), 149–154. https://doi.org/10.3758/PBR.17.2.149

Goethe, O., Sørum, H., & Johansen, J. (2021). The effect or non-effect of virtual versus non-virtual backgrounds in digital learning. In T. Ahram, & R. Taiar (Eds.), *Lecture notes in networks and systems: Vol. 319. Human interaction, emerging technologies and future systems* (pp. 274–281). Springer. https://doi.org/10.1007/978-3-030-85540-6_35

Granot, Y., Feigenson, N., Balcetis, E., & Tyler, T. (2018). In the eyes of the law: Perception versus reality in appraisals of video evidence. *Psychology, Public Policy, and Law*, *24*(1), 93–104. https://doi.org/10.1037/law0000137

Hans, V. P. (2022). Virtual juries. *DePaul Law Review*, *71*(2), 301–330. http://dx.doi.org/10.2139/ssrn.3860165

Hwang, A. H.-C., Wang, C. Y., Yang, Y.-Y., & Won, A. S. (2021). Hide and seek: Choices of virtual backgrounds in video chats and their effects on perception. In *Proceedings of the ACM on Human-Computer Interaction* (Vol. 5, Iss. CSCW2, pp. 1–22). New York, NY. https://doi.org/10.1145/3476044

Legg, M., & Song, A. (2021). The courts, the remote hearing and the pandemic: From action to reflection. *University of New South Wales Law Journal*, *44*(1), 126–166. https://doi.org/10.53637/ZATE4122

Machado, M., Sousa, M., Rocha, V. & Isidro, A. (2018). Innovation in judicial services: a study of innovation models in labor courts. *Innovation & Management Review*, *15*(2), 155–173. https://doi.org/10.1108/INMR-04-2018-010

Meredith, R., David, T., & McCurdy, M. (2021). Justice reimagined: challenges and opportunities with implementing virtual courts. *Current Issues in Criminal Justice*, *33*(4), 1–17. https://doi.org/10.1080/10345329.2020.1859968

Mohamad, A. M., & Sule, I. (2021). ICT-Enabled Applications for Decision-Making by the Courts: Experiences from Malaysia and Nigeria. *International Journal of Law, Government and Communication*, *6*(22), 189–196. https://doi.org/10.35631//ijlgc.6220018

Nir, E., & Musial, J. (2022). Zooming in: Courtrooms and defendants' rights during the COVID-19 pandemic. *Social & Legal Studies*, *31*(5), 725–745. https://doi.org/10.1177/09646639221076099

Olubukola, O., & Abimbola, D. (2022). Remote Court Proceedings in Nigeria: Justice Online or Justice on the Line. *International Journal for Court Administration*, *13*(2), 21–38. https://doi.org/10.36745/ijca.448

Rossner, M. (2021). Remote rituals in virtual courts. *Journal of Law and Society*, *48*(3), 334–361. https://doi.org/10.1111/jols.12304

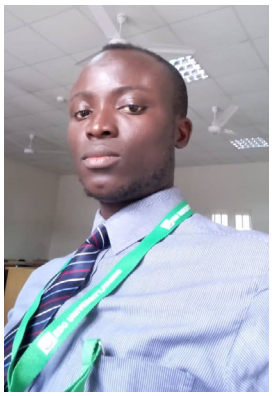
Sanson, M., Crozier, W. E., & Strange, D. (2020). Court case context and fluency-promoting photos inflate the credibility of forensic science. *Zeitschrift für Psychologie*, *228*(3), 221–225. https://doi.org/10.1027/2151-2604/a000415

Tait, D., & Tay, V. (2019). *Virtual court study: Report of a pilot test 2018*. Western Sydney University. https://doi.org/10.26183/5d01d1418d757

Thornburg, E. G. (2021). Observing online courts: Lessons from the pandemic. *SSRN Electronic Journal*, *54*(3), 181–244. https://doi.org/10.2139/ssrn.3696594

Winter, B., Daguna, J., & Matlock, T. (2018). Metaphor-enriched social cognition and spatial bias in the courtroom. *Metaphor and the Social World*, *8*(1), 81–99. https://doi.org/10.1075/msw.17001.win

Информация об авторах



Айдоноджи Пол Атагамен – PhD, преподаватель права, координатор отдела аспирантуры, факультет права, Государственный университет Эдо-Узайруэ
Адрес: 689M+PP5, 312107, Нигерия, штат Эдо, г. Иямхо, Аучи/Абуджа Экспресс Вей
E-mail: aidonojie.paul@edouniversity.edu.ng
ORCID ID: https://orcid.org/0000-0001-6144-2580
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57221636261
Google Scholar ID: https://scholar.google.com/citations?user=0h9E2ZIAAAAJ

Вакили Самину Абача – ассистент исследователя, факультет права, Государственный университет Эдо-Узайруэ
Адрес: 689M+PP5, 312107, Нигерия, штат Эдо, г. Иямхо, Аучи/Абуджа Экспресс Вей
E-mail: wakili18.saminu@edouniversity.edu.ng
ORCID ID: https://orcid.org/0009-0000-7043-286X

Аюба Давид – ассистент исследователя, факультет права, Государственный университет Эдо-Узайруэ
Адрес: 689M+PP5, 312107, Нигерия, штат Эдо, г. Иямхо, Аучи/Абуджа Экспресс Вей
E-mail: ayuba18.david@edouniversity.edu.ng
ORCID ID: https://orcid.org/0009-0008-7706-9627

Вклад авторов

Пол А. Айдоноджи осуществлял общее руководство и постановку задач исследования; поиск и подбор научной литературы; критическую оценку интерпретации результатов исследования; формулировку ключевых выводов, предложений и рекомендаций; утверждение окончательного варианта статьи.
Самину А. Вакили проводил анализ национального законодательства; выполнял интерпретацию результатов исследования; организовал проведение социологического опроса и подготовку черновика рукописи.
Давид Аюба занимался сбором и анализом литературы и законодательства; проводил социологический опрос; выполнял интерпретацию результатов исследования; осуществлял подготовку чистовика рукописи.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.91 / Государство и право отдельных стран
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 18 августа 2023 г.
Дата одобрения после рецензирования – 25 октября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.