CHALLENGES TO IMPLEMENTING THE INTERNATIONAL DIGITAL LAW TO PROTECT DIGITAL RIGHTS

Abeer Alubaidi

ABSTRACT

Objective: In the ongoing digital era, digital rights are a major concern and demand measures to address challenges that encompass the management of effective law implementation. The following study aims at the contrivance and administration of international law to address digital rights.

Method: Legal aspects of digital technology, also known as information technology law, is a practical field of law that has established a strong position among other legal fields in recent years, both in legal firms and educational institutions. Fresh technological advancements like massive data, the Web of Things, quantum computation, distributed ledger technology, and advanced formulas provoke inquiries concerning the governance of these technologies, such as the entitlements and safeguards that individuals possess or ought to possess. The growing utilization of electronic technologies by corporations and governments prompts various inquiries concerning the management of these technologies, specifically concerning the privileges and lawful safeguards individuals have a claim to.

Result: The emphasis is primarily on the utilization and possible alteration of current (basic) entitlements. Nevertheless, the argument and lawful exploration in this domain needs a more extensive conversation regarding the novel entitlements that individuals ought to possess in the digital epoch. Occasionally, novel ideas emerge, like the concept of the 'right to erasure'.

Conclusion: This piece of writing discusses the inquiry of what fresh, supplementary entitlements could be envisioned in the age of technology if we were to compose them anew, without being restricted to a predetermined collection of essential liberties. To initiate a more extensive lawful discussion on this matter, several novel entitlements for individuals in the electronic sphere are suggested.

Keywords: international digital law, digital rights, challenges, implementing, protection, cyber-security, data privacy, jurisdiction, harmonization, cross-border cooperation, enforcement mechanisms, global standards, cultural differences, technological advancements, legal frameworks, internet governance, surveillance, digital sovereignty, corporate influence, education and awareness.

Received: 29/05/2023
Accepted: 22/08/2023
DOI: https://doi.org/10.55908/sdgs.v11i5.554

* PhD in International Law, School of Law, Al Taif University, Saudi Arabia, E-mail: ab.alubaidi@gmail.com, Orcid: http://orcid.org/0000-0001-9339-0201
DESAFIOS À APLICAÇÃO DO DIREITO INTERNACIONAL DIGITAL PARA PROTEGER OS DIREITOS DIGITAIS

RESUMO

Objetivo: Na era digital em curso, os direitos digitais são uma grande preocupação e exigem medidas para enfrentar os desafios que englobam a gestão da implementação efetiva da lei. O estudo a seguir visa o artifício e a administração do Direito Internacional para abordar os direitos digitais.

Método: Aspectos legais da tecnologia digital, também conhecida como lei de tecnologia da informação, é um campo prático do direito que estabeleceu uma posição forte entre outros campos legais nos últimos anos, tanto em escritórios jurídicos e instituições educacionais. Avanços tecnológicos recentes como dados massivos, a Web of Things, computação quântica, tecnologia de livro-razão distribuído e fórmulas avançadas provocam questionamentos sobre a governança dessas tecnologias, tais como os direitos e salvaguardas que os indivíduos possuem ou deveriam possuir. A crescente utilização de tecnologias eletrônicas por empresas e governos leva a várias perguntas sobre a gestão dessas tecnologias, especificamente no que diz respeito aos privilégios e salvaguardas legais que os indivíduos têm direito a.

Resultado: A tônica é colocada principalmente na utilização e eventual alteração dos direitos atuais (de base). No entanto, o argumento e exploração legal neste domínio precisa de uma conversa mais extensa sobre os novos direitos que os indivíduos devem possuir na época digital. Ocasionalmente, surgem novas ideias, como o conceito do “direito ao apagamento”.

Conclusão: Este texto discute a indagação de que direitos novos e complementares poderiam ser imaginados na era da tecnologia se fôssemos reconstituir, sem ficar restritos a uma coleção predeterminada de liberdades essenciais. Para iniciar uma discussão legal mais ampla sobre esta matéria, vários novos direitos para os indivíduos na esfera eletrônica são sugeridos.

Palavras-chave: direito digital internacional, direitos digitais, desafios, implementação, proteção, segurança cibernética, privacidade de dados, jurisdição, harmonização, cooperação transfronteiriça, mecanismos de aplicação, normas globais, diferenças culturais, avanços tecnológicos, quadros jurídicos, governança da internet, vigilância, soberania digital, influência corporativa, educação e conscientização.

1 INTRODUCTION

The execution of a global electronic statute to safeguard electronic entitlements is confronted with myriad obstacles that necessitate meticulous contemplation and tactical methodologies. In a progressively interconnected globe, where the electronic domain performs a crucial function in our day-to-day existence, securing electronic privileges has turned into an urgent apprehension. This presents the necessity for an all-inclusive lawful structure that deals with concerns like cyber protection, information confidentiality, territoriality, and execution methods on an international level. One of the main obstacles involves creating efficient systems to safeguard people's virtual entitlements while weighing the concerns of authorities, enterprises, and consumers. Cybersecurity menaces persist in developing, with malevolent performers taking advantage of susceptibilities in
machinery and systems. Creating resilient metrics to protect digital infrastructure and individual information is crucial to upholding confidence in the digital environment. Yet another noteworthy hindrance is the synchronization of regulations amidst diverse territories. The worldwide characteristic of the electronic realm demands a consolidated strategy, however, diverse juridical frameworks, ethnic disparities, and opposing concerns may obstruct the establishment of harmonized principles. Equilibrating the requirement for worldwide collaboration with the conservation of territorial autonomy poses a complicated predicament that needs to be tackled in the execution of global digital legislation.

Implementation methods present an additional significant obstacle. Electronic privilege breaches frequently go beyond boundaries, rendering it challenging to incriminate wrongdoers. Establishing efficient transnational collaboration and surrender protocols is vital to guarantee that individuals who violate digital entitlements can be held accountable, irrespective of their whereabouts. Scientific progressions are additionally intricate to the execution of electronic regulations. The swift speed of novelty frequently surpasses the establishment of lawful structures, creating difficulties for statutes to stay abreast of budding technologies. Preemptive actions are imperative to foresee and tackle possible hazards linked with novel technologies, like machine learning, distributed ledger, and the Web of Things.

Furthermore, the impact of influential enterprises in the virtual realm presents both possibilities and obstacles. Achieving equilibrium amidst safeguarding digital entitlements and facilitating novelty necessitates tackling concerns associated with business sway, monopolistic maneuvers, and the conscientious utilization of information. Guaranteeing that digital entitlements are not jeopardized in preference of business concerns necessitates meticulous scrutiny of corporate methodologies and efficient regulatory supervision.

Learning and consciousness furthermore have a crucial function in the prosperous execution of worldwide electronic regulation. Advancing electronic proficiency and enabling persons to comprehend their entitlements and obligations in the electronic realm is pivotal. Augmenting communal cognizance and involvement may cultivate an ethos of cyber entitlements promotion, generating a further knowledgeable and authorized populace.
2 THEORETICAL FRAMEWORK

2.1 DEFINITION OF INTERNATIONAL DIGITAL LAW

Global electronic legislation pertains to a collection of lawful concepts, guidelines, and statutes that oversee the utilization, safeguarding, and entitlements linked with electronic technology and the electronic domain on a worldwide level. It covers an extensive array of lawful concerns, comprising cyber safety, information confidentiality, intangible asset entitlements, territorial affairs, intercontinental collaboration, and the management of computerized undertakings. Global digital legislation endeavors to create a structure that encourages the safeguarding of people's digital entitlements enables worldwide collaboration, and guarantees uniformity of regulations in the digital realm, considering the intricacies that emerge from the worldwide character of the digital milieu and the interdependence of digital operations across international frontiers.

2.2 IMPORTANCE OF PROTECTING DIGITAL RIGHTS

Safeguarding electronic entitlements is of utmost significance in the present-day highly developed universe. Here are some primary rationales why protecting digital entitlements is vital: Confidentiality and Individual Self-determination: Cyber entitlements preservation guarantees persons possess authority over their private data, internet undertakings, and virtual personas. It enables people to make knowledgeable decisions regarding the gathering, utilization, and distribution of their information, conserving their confidentiality and individual independence.

Liberty of Articulation: The online domain has turned into a vital stage for people to articulate their viewpoints, distribute knowledge, and participate in civic conversations. Safeguarding digital entitlements, like liberty of expression and entry to knowledge, is crucial for maintaining democratic principles and empowering a lively, comprehensive, and multifarious cyberspace.

Cybersecurity and Information Preservation: Cyber perils, such as breaching, data violation, and personality stealing, present noteworthy hazards to persons, establishments, and even state security. Sturdy digital entitlements safeguarding aids in setting up norms and gauges to boost cyber safety, shield confidential data, and defend against unapproved entry and malevolent undertakings.

Novelty and Financial Expansion: Cyber entitlements safeguarding nurtures a milieu that stimulates novelty, ingenuity, and enterprise. Through the protection of
intellectual property privileges and encouragement of equitable rivalry, it encourages financing in exploration and innovation, provokes scientific progress, and propels financial expansion in the digital domain.

Communal Equivalence and Incorporation: Entrance to electronic technologies and internet amenities has transformed into an essential component of engaging in contemporary civilization. Safeguarding electronic entitlements guarantees equitable admittance and possibilities for every person, irrespective of their socioeconomic status, sex, race, or geographic area. It aids in connecting the technological gap and encourages communal integration.

The lawful and moral structure: Safeguarding digital rights institutes a lawful and moral structure that regulates digital pursuits, establishes benchmarks for conscientious conduct, and makes individuals, groups, and administrations answerable for their deeds in the digital domain. It assists in guaranteeing that essential privileges and principles are maintained in the swiftly developing electronic terrain.

Faith and Assurance: Maintaining electronic entitlements fosters an atmosphere of reliance and faith amidst users, enterprises, and administrations. When people perceive that their digital entitlements are honored and safeguarded, they are more likely to partake in internet undertakings, exchange data, and take part in the electronic marketplace, adding to a flourishing and dependable digital habitat.

To recapitulate, safeguarding digital entitlements is crucial for conserving confidentiality, empowering liberty of speech, amplifying cyber safety, cultivating novelty, advocating for communal impartiality, instituting lawful and moral structures, and constructing reliance in the cyber realm. By maintaining electronic privileges, we can establish a comprehensive, safe, and rights-honoring electronic atmosphere that advantages individuals, communities, and financial systems as a complete.

3 METHODOLOGY

A brief overview of the challenges in implementing the law: Enforcing electronic regulations to safeguard electronic entitlements presents various obstacles that require resolution. Several primary obstacles comprise:

1. **Territorial Complication:** The virtual domain surpasses country borders, creating difficulties in ascertaining legal authority and implementing regulations.
Electronic undertakings frequently encompass numerous territories, necessitating global collaboration and unification of lawful structures.

2. **Technological Progress**: The swift speed of technological progress surpasses the establishment of lawful structures. Fresh technologies, like machine learning and distributed ledger, present new lawful hurdles that necessitate forward-thinking and flexible methods.

3. **Cultural and Juridical Heterogeneity**: Diverse nations exhibit dissimilar cultural conventions and juridical frameworks, rendering it arduous to institute worldwide benchmarks. Connecting the divides amidst diverse cultural and juridical frameworks is crucial for efficient execution of global digital regulations.

4. **Implementation and Responsibility**: Guaranteeing efficient implementation systems for cyber regulations is intricate. Electronic privilege breaches frequently happen beyond frontiers, and recognizing and penalizing wrongdoers can be demanding. Enhancing global collaboration and establishing resilient systems for inquiry and litigation are pivotal.

5. **Equilibrating Confidentiality and Safety**: Safeguarding cyber entitlements necessitates achieving a subtle equilibrium amid confidentiality and safety. Whilst ensuring the protection of private information is crucial, authorities and institutions must also tackle cyber threats to safeguard citizens and the welfare of the country.

6. **Business Control**: Dominant enterprises in the online realm have the ability to sway policies and rules. Equilibrating the concerns of enterprises with the safeguarding of personal liberties necessitates sturdy regulatory structures and supervision systems to avert monopolistic behaviors and guarantee conscientious utilization of information.

7. **Learning and consciousness**: Advocating technological proficiency and elevating cognizance regarding technological entitlements are crucial obstacles. Numerous people might not possess a complete understanding of their entitlements or the probable hazards in the virtual realm. Teaching and enabling individuals to comprehend and support their online entitlements is vital.

8. **Global Collaboration**: Executing worldwide digital regulations necessitates collaboration amid countries with diverse preferences and schedules.
Constructing agreement, nurturing teamwork, and creating efficient avenues of correspondence and harmony are crucial for prosperous execution.

Tackling these obstacles necessitates all-encompassing methodologies that entail cooperation amid administrations, groups, non-governmental establishments, and persons. It encompasses forward-thinking adjustment to technological progress, transnational collaboration, synchronization of lawful structures, and a dedication to safeguarding and maintaining online entitlements in a swiftly changing digital terrain.

**The Changing Landscape - Digital Human Rights:** Despite the fact that human rights theory typically portrays human rights as pre-political, infused with inherent law characteristics, such as principles derived from natural rights ideology, spiritual convictions, unadulterated logic, or purported human capacities, these concepts are not universal and are limited by time and place. The Routledge Encyclopedia of Philosophy (Human Rights Edition, 2006)

International human rights law (IHRL) has evolved throughout time to include new considerations, each time and place having its own unique legal, political, economic, technical, and social context. Several Authors (2023) This is because the development of international law depends on individual political "acknowledgments" carried out through the implementation of lawful particular instruments and through actual state conduct, and is thus shaped as much by pragmatic considerations about the actual needs and desires of political groups as by lofty theory about what the substance of human rights law ought to be. As a result, it is not surprising that Vasak was able to place his "three generations of IHRL" classification in distinct historical epochs,(Karel Vasak, A 30-Year Struggle, 1997) aligning with momentous political, economic, technological, and cultural advancements such as revolutions against autocratic rulers or external monarchs inspired by ideas from the era of illumination, the establishment of a social security system after the industrial revolution, and the liberatio. Just as the Universal Declaration of 1948, which primarily serves as a prescriptive guide for the global human rights campaign, explicitly addressed certain distinct societal and technological obstacles of that era, such as guaranteeing access to media beyond borders, protecting labor associations, and fostering scientific instruction, so too does the Declaration of Human Rights of 1960. (House Resolution 217, Third Reading) The Agreements of 1966, which addressed essential features of modern social-democratic states such as the need to build a framework for
community policy and to ensure equal and emancipated intermittent elections, may be said in the same way. Reference: (Article 9 of the International Covenant on Economic, Social, and Cultural Rights, cited in Note 2 above)

A social acknowledgement process had taken place in every occasion when global declarations and agreements had been expressed and accepted. Throughout these actions, human rights were transformed from abstract ethical conceptions or claims into a set of legally binding rights and obligations, or in the case of adaptable legal instruments, into measurable society expectations and strategic recommendations. Such transformational acts are usually adaptable to the varying needs and expectations of various groups, as well as to the innovative risks and challenges that people and societies face as a result of the ever-evolving economic, technical, and cultural conditions. They are also susceptible to actual historical experiences of power abuse and injustice, which encourage the introduction of innovative entitlements that are often conceived to benefit individuals and groups at the expense of governmental institutions.

Debatably, the modern "electronic upheaval" and its associated branches signify yet another technological advancement with significant economic, political, and cultural consequences. Similar to previous instances, this uprising also welcomes a procedure of normative alteration encompassing the conversion of theoretical notions regarding "cyber entitlements" or "guidelines for the digital era" into tangible legally-acknowledged human rights standards via a process of legal interpretation and legislation - that is, through the expression of novel legally binding or non-binding legal instruments. The UN Human Rights Council and General Assembly have tackled the task of adjusting IHRL to the digital era by embracing a plethora of non-binding resolutions that endorse the expansion of offline human rights to activities and interactions on the internet.

The EU Commission has additionally released a Proclamation on Digital Rights and Principles for the Digital Era in which it undertook the essential measures to guarantee reverence for the privileges of individuals both offline and online. This

---

2 KLAUS SCHWAB, THE FOURTH INDUSTRIAL REVOLUTION 3 (2017). Among the offshoots of the digital revolution one can mention the connectivity revolution, the AI revolution, the big data revolution, the cloud revolution and their fusion with other new technologies, such as blockchain, natural language processing, and biometrics.

strategy evades the notion of the online realm as an IHRL-free "abyss," and perpetuates a time-honored practice of adapting prevailing human rights to novel and evolving societal circumstances.\(^4\)

To ensure, the process of adjustment of old IHRL norms to new situations occasionally necessitates incorporating substantial alterations in the extent and substance of pre-existing IHRL norms and in the approach of their implementation to previously unanticipated circumstances. For instance, there is minimal uncertainty that the fundamental justifications endorsing liberty of speech are applicable both offline and online,\(^{10}\) and that safeguarding the globally acknowledged entitlement to receive and convey information, "via any means," should encompass the distribution of materials on social networking sites and alternative digital platforms. However, the diverse societal and technological circumstances for the practice of liberty of speech in a digital setting might encourage a more robust regulatory reaction, particularly concerning objectionable language. That might be imperative owing to the heightened perils associated with internet vitriol (arising from variances in the velocity, extent, and magnitude of the spread of detrimental online materials), and the evident "shortcoming" of the digital "forum of thoughts" to adequately tackle the issue of misinformation (partially due to the distorting impacts of algorithmic filter bubbles and echo chambers that foster motivations to circulate contentious content).\(^5\)

Occasionally, the adjustment of the extent and substance of offline privileges to an online setting might necessitate the formulation of novel theoretical validations for the entitlement in query. For instance, hypotheses concerning the entitlement to internet confidentiality unveil a shift from safeguarding individuals against unwarranted encroachment of their secluded and intimate domains to safeguarding and overseeing personal data in both secluded and communal environments. Suppositions concerning confidentiality must progressively contemplate how to safeguard individuals against unwarranted manipulation of their desires, cognitions, and viewpoints. (Marcello Ienca & Roberto Andorno)

However, in certain instances, the prescriptive disparity between offline human rights and the necessities and desires of internet users reaches a worrisome

---

\(^4\) Vasak, supra note 3; see also SAMUEL MOYN, THE LAST UTOPIA: HUMAN RIGHTS IN HISTORY 225 (2010).

\(^5\) Dror-Shpoliansky & Shany, supra note 7, at 1266–267; see also Tomer Shadmy, Content Traffic Regulation: A Democratic Framework to Address Misinformation, 63 JURIMETRICS 1 (2022).
magnitude, indicating that modification of an established entitlement is no longer viable or would result in "desperately insufficient" outcomes. In those situations, the emergence of novel human rights—such as the privilege to not be subjected to algorithmic determinations or the entitlement to be erased—might be justified.⁶

Traversing amidst ancient and novel standards entails challenging lawful strategy predicaments. Establishing novel standards of International Human Rights Law (IHRL) does not inevitably necessitate the implementation of a fresh IHRL structure, but it highlights the deficiencies of the current framework. However, recognizing the inappropriateness of current offline privileges without there being an easily accessible novel collection of human privileges to provide safeguard to internet users generates the danger that individuals would be left neither here nor there—i.e., confronting a safeguard void. Simultaneously, adhering to the current IHRL standards, despite their growing perception as unsuitable, also leads to insufficient safeguarding of digital necessities and concerns. Even more dire, it transmits to states, tech firms, and other stakeholders a perilously comforting message that they can persist in a "status quo" mode of operation.

However, there are specific facets of digital human rights that encourage a reassessment of certain fundamental characteristics of international human rights law (IHRL): The prevalence of the territorial pattern for the implementation of human rights commitments; the emphasis on accountability of governments for human rights transgressions, as opposed to multinational corporations and other non-state entities; and the inclination of IHRL bodies to employ IHRL instruments independently from other legal instruments. This article examines the degree to which crucial ethical and organizational reactions to the difficulties presented by the digital era are harmonious with, or engage with, alterations in the aforementioned pivotal characteristics of the current IHRL structure. Indeed, this article asserts that the IHRL framework is already evolving in this aspect, partially owing to its interaction with digital human rights. These emerging transformations may generate fresh possibilities for advocating human rights in the digital era and might make the policy decision between alteration and steadiness of IHRL—inconsequential. Simultaneously, the shifting prescriptive terrain might provoke fresh apprehensions regarding the

⁶ Regulation (EU) 2016/679 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 (General Data Protection Regulation), art. 21, OJ L 119/1 (2016) [hereinafter GDPR].
governmental permissibility of -IHRL- to nations. After this preamble, Section B will elucidate the evolution of digital human rights, employing the "three iterations" classification that I have formulated elsewhere (in collaboration with Daphna Dror-Shpoliansky). (Dror-Shpoliansky & Shany, supra note 7.) Section C will elucidate how novel advancements in the realm of digital human rights align with wider advancements in IHRL, encompassing the extraterritorial implementation of human rights, responsibilities on governments to actively supervise private enterprises, and the deterioration of normative frontiers demarcating distinct human rights conventions from other facets of IHRL and global law.

**The Three Generations of Digital Human Rights:** I have proposed elsewhere—in an article co-authored with Dafna Dror Shpoliansky—that IHRL organizations and stakeholders have a tendency to react to the difficulties faced by the rights and requirements of internet users caused by innovative digital technology through three main categories of reactions, which can be characterized as embodying three "epochs" of digital human rights. The inaugural era encompasses a revolutionary reevaluation of prevailing human entitlements to enable their alignment with the novel circumstances of the digital era. The subsequent iteration encompasses the formation of novel digital human rights, corresponding to the fresh requirements and concerns of internet users. These subsequent iteration privileges have no nearby counterparts in the physical realm. The tertiary era encompasses the acknowledgment of novel entitlement-holders and fresh obligation-holders.

The initial era of digital entitlements entails a vibrant reevaluation of certain fundamental components constituting the description of pertinent offline entitlements, a fresh methodology towards their implementation, and, occasionally, a novel doctrine validating the presence of the entitlement in query. This subsequent expansion suggests that inaugural era privileges might, in certain aspects, be the perpetuation solely in designation of the authentic offline entitlement. Online liberty of speech, referenced earlier, is one exemplification of a primary era digital entitlement. The extent of the privilege has been broadened by global organizations to encompass online communication, and it has been contended that this digitally-altered privilege to liberty of expression now includes a derived privilege to connect

---

to the Internet. Simultaneously, the implementation of restrictions to autonomy of speech has been championed by human rights office bearers more vehemently than previously, considering the distinct way in which objectionable material is spread on the internet and the distorting influence on societal conversation caused by online misinformation. Because of the escalated peril linked with offensive online language, digital platforms have been urged by states and global organizations to formulate and implement efficient content moderation regulations. The transition from the customary hands-off stance of IHRL organizations, which were typically doubtful towards speech control by governments, to a more supportive regulatory position, also demonstrates a modification in the theoretical presumptions underlying freedom of speech and a fundamental alteration in social circumstances. In the offline realm, the prevailing state was that of knowledge shortage, which indicated a necessity to unleash additional data into a somewhat disorganized marketplace of concepts and knowledge. However, in the virtual realm, the model seems to encompass an abundance of data wherein socially detrimental content could overshadow socially advantageous information. The outcome of this has been an assertion in support of organizing preemptively an efficient marketplace of concepts and knowledge. This would entail regulation that guarantees that information distributed online will be favorable to a well-educated and cultured public dialogue. (Cf. Saskatchewan (Human Rights Commission) v. Whatcott, [2013])

Another illustration of a primary-era digital human entitlement is the privilege to internet confidentiality. Here, also, the substance of the right has experienced numerous alterations, just as its method of implementation and fundamental doctrine. For instance, the focal point of legal practices focused on safeguarding the entitlement to confidentiality has transitioned from safeguarding individuals against encroachments of their private intimate areas to safeguarding their individual information. Now, with the surge of colossal data, the emphasis has shifted even further from safeguarding data classified as "confidential" in essence towards safeguarding all recognizable data, including publicly accessible data, from which confidential data can be extracted. These advancements in law-interpretation and

---

law-application are endorsed, as previously mentioned, by a shift in the ideology underpinning privacy. The hypothetical alteration entails a transition from a prevailing perception of privacy as a privilege to be solitary, to ideas of privacy encompassing the privilege to exert authority over personal information and its resultant applications, including managing interpersonal data streams and deterring endeavors to influence individuals' cognitive processes.10

Similar to primary generation rights, secondary generation rights can also be enforced within the current IHRL framework. The disparity between the two generations is that the preceding one encompasses, at the very least, the invocation of preexisting offline entitlements, while the subsequent one involves the introduction of novel digital entitlements. Among privileges suggested or genuinely evolved as part of this advancement, one may cite the subsequent: An autonomous novel entitlement to access the Internet, (Internet Governance Forum) which originates from a comprehension of entry to the Internet as a prerequisite for the enjoyment of a wide array of digital rights and interests (surpassing the conventional right to search, receive, and convey information); a fresh entitlement to informational self-governance, which recognizes that the manner of portrayal of personal information online constitutes an expansion of the human person and should be effectively managed by the relevant data subject; and the new entitlement not to be subjected to automated decisions in significant matters, which safeguards the right and interest of individuals to be liberated from arbitrary and non-accountable exercise of de facto power through algorithms and to exist in a non-datafied form.11

These initial and subsequent generation human rights do not necessitate a formal alteration in the IHRL framework. Nevertheless, they persist in significant strain with that structure. This is due to the pleasure of digital privileges being greatly reliant on the behavior of private enterprises—particularly Internet service providers and online Internet platforms. The enterprise framework and technology these corporations employ might have a greater influence on the capacity to relish digital human entitlements than governmental oversight. The repercussions of this personal behavior can stretch to determining entry to online platforms; to the gathering,

preservation, and retrieval of individual data; to directing the distribution of information to specific individuals; to the promotion of data transferability; and to choices concerning content regulation guidelines, distinct confidentiality, and algorithmic openness. However, notwithstanding the novel privatized actuality governing the pleasure of entitlements, IHRL organizations persist in concentrating on scrutinizing the lawfulness of governmental behavior rather than the commercial activities of private enterprises. Moreover, since technology corporations typically function on a worldwide scale, utilizing global supply chains and infrastructure locations, their reliance on any specific host or domicile state could be negligible. Inherently, this constrains states’ capacity to, and inclination towards, regulating these corporations’ endeavors. Consequently, the framework of indirect oversight of enterprises to promote human rights considerations, a framework that revolves around tackling the governing and judicial authorities of the pertinent nations, has restricted traction in the tangible realm of digital technology. (David Bilchitz, 2013)

**Lack of strong enforcement mechanisms:** One of the noteworthy hurdles in executing digital regulations to safeguard digital entitlements is the deficiency of robust implementation methods. Whilst statutes and rules may be present, guaranteeing their efficient implementation can prove to be difficult in the virtual domain. Electronic privileges breaches frequently transpire beyond frontiers, causing complexity in recognising and penalising wrongdoers. The territorial intricacies and diverse judiciary frameworks additionally convolute implementation endeavours. Furthermore, the ever-changing and swiftly progressing characteristic of technology frequently surpasses the progression of enforcement actions, generating a disparity between the legislation and its pragmatic execution. Enhancing global collaboration, enhancing transnational synchronisation, and establishing resilient systems for enquiry, indictment, and sanctions are crucial to surmount the obstacles and guarantee efficient implementation of cyber liberties legislations. Lacking robust implementation tools, the efficacy of digital regulations in safeguarding people’s entitlements in the virtual realm could be considerably reduced.

The execution of electronic regulations to safeguard electronic entitlements confronts numerous obstacles, such as the complexity in recognising accountable entities, the restricted authority of domestic regulations, and an absence of global collaboration.
Challenge in recognising accountable individuals: In the virtual domain, it may be difficult to track and assign actions to particular persons or organisations implicated in digital liberties breaches. The obscurity and alias granted by the internet setting, coupled with the utilisation of advanced methods to conceal identities, create challenges in pinpointing and penalising those liable for violations. This difficulty impedes the efficient implementation of cyber regulations.

Restricted scope of federal regulations: Electronic pursuits frequently surpass geographical borders, creating difficulties for singular nations to establish authority and implement their regulations efficiently. The worldwide characteristic of the internet and the unrestricted nature of digital platforms imply that digital entitlements breaches can transpire outside the grasp of a nation’s lawful structure. This constraint generates lawful ambiguities and openings in the safeguarding of electronic entitlements, since domestic regulations might not hold sway over deeds emanating from beyond their border.

Deficiency of global collaboration: Electronic privileges safeguarding necessitates sturdy global teamwork and partnership. Nonetheless, disparities in lawful frameworks, clashing territorial demands, and divergent preferences among nations may impede efficient collaboration. Reciprocal lawful support systems and global pacts might be present, however, the deficiency of uniform and all-inclusive collaboration structures can hinder the prompt and effective settlement of transnational digital entitlements infringements. The nonexistence of uniform methods and mutual strategies may generate difficulties in coordinating endeavours and implementing electronic regulations collectively.

Conflicting national laws and policies: Contradictory domestic regulations and strategies pose a noteworthy obstacle in executing electronic regulations to safeguard electronic entitlements. Diverse nations frequently possess their individual lawful structures and strategies concerning electronic operations, information preservation, and internet administration. These laws and policies can vary significantly, leading to inconsistencies, conflicts, and legal uncertainties in the global digital landscape. Contradictory domestic regulations may generate ambiguity for persons, groups, and online platform suppliers who function transnationally. It can hinder cross-border data flows, impede international cooperation, and result in gaps in the protection of digital rights. Concerted endeavours, global accords, and cooperative methodologies are
imperative to tackle these clashes, advance uniformity, and guarantee the efficacious safeguarding of virtual entitlements on a worldwide scale.

**Differences in definitions of digital rights:** Variations in explanations of electronic entitlements, opposing rules in diverse nations, and the challenge in unifying statutes and strategies are noteworthy obstacles in executing digital regulations to safeguard digital entitlements.

Disparities in explanations of electronic entitlements emerge because of fluctuations in juridical frameworks, customary conventions, and communal principles throughout nations. As an instance, whereas certain nations might give precedence to liberty of speech as a crucial online entitlement, others might lay more significance on safeguarding national safety or preserving communal harmony. These discrepancies in explanations may impede the creation of a mutual comprehension and structure for safeguarding digital entitlements, rendering it difficult to formulate unified and uniform global criteria.

**Conflicting regulations in different countries:** Variations in explanations of electronic entitlements, opposing rules in diverse nations, and the challenge in unifying statutes and strategies are noteworthy obstacles in executing digital regulations to safeguard digital entitlements.

Disparities in explanations of electronic entitlements emerge because of fluctuations in juridical frameworks, customary conventions, and communal principles throughout nations. As an instance, whereas certain nations might give precedence to liberty of speech as a crucial online entitlement, others might lay more significance on safeguarding national safety or preserving communal harmony. These discrepancies in explanations may impede the creation of a mutual comprehension and structure for safeguarding digital entitlements, rendering it difficult to formulate unified and uniform global criteria.

**Difficulty in harmonizing laws and policies:** The complexity of reconciling regulations and strategies contributes to the obstacles of safeguarding online entitlements. Concordance necessitates global teamwork and partnership to synchronise lawful structures and strategies throughout nations. Nevertheless, attaining agreement can be intricate because of the varied concerns, preferences, and judicial customs of distinct countries. Inconsistencies in domestic statutes, diversity in customs, and differing degrees of technological advancement additionally complicate the endeavour of synchronisation,
rendering it difficult to institute a globally relevant lawful structure for safeguarding digital entitlements.

These obstacles in the execution of electronic regulations to safeguard electronic entitlements underscore the necessity for global collaboration, discourse, and endeavours to connect the disparities between diverse lawful frameworks and societal backgrounds. It necessitates constructing agreement, nurturing comprehension, and discovering shared territory to establish synchronised structures that maintain essential online entitlements tenets while acknowledging the distinct attributes and requirements of particular nations. Such undertakings may aid in surmounting the obstacles presented by variances in interpretations, opposing statutes, and the challenge of unifying regulations and protocols, resulting in enhanced safeguarding of digital entitlements worldwide.

3.1 DIGITAL RIGHTS AND CHANGES IN IHRL

The traditional structure of International Human Rights Law (IHRL) principles, which can be traced back to the 1948 Universal Declaration of Human Rights, has predominantly centred its attention on delineating the intricate dynamics between governing bodies and the diverse array of individuals and groups that fall within their jurisdictional purview. The primary goal of this initiative is to effectively address and mitigate the pervasive issue of governmental abuse of power. By doing so, it aims to safeguard and protect the fundamental rights and liberties that every individual is entitled to. This abuse of power, if left unchecked, has the potential to significantly hinder and obstruct the ability of the general populace to fully enjoy and exercise their basic rights. Therefore, this initiative seeks to establish a robust framework that effectively curbs and prevents such abuses, ensuring that governments operate within the confines of the law and respect the rights of their citizens. When considering the nature of states and their administrations, it becomes evident that their fundamental characteristics revolve around territorial dominion and authority. As a result, the conventional approach to International Human Rights Law (IHRL) has consistently prioritised and emphasised the concept of territoriality. When examining the dynamics of the interaction between a government and its population, it is important to consider that this interaction predominantly occurs within the confines of the geographical borders of the respective nation. This means that the relationship between a government and its citizens is primarily established
and maintained within the territorial boundaries of the nation-state. This localised context plays a significant role in shaping the nature and extent of the interaction, as it creates a distinct framework within which the government operates and the population engages with the governing authorities. By recognising the spatial dimension of this interaction, we gain a deeper understanding of how governments and populations interact. In addition to this, it is worth noting that the traditional approach to International Human Rights Law (IHRL) has predominantly centred its attention on the regulation of governmental conduct. This approach, whether implicitly or explicitly, acknowledges that governments can potentially be responsible for violating human rights. One of the notable aspects of international human rights law (IHRL) is its relatively limited geographical scope. This means that IHRL primarily focuses on the protection and promotion of human rights within specific territories or regions. In comparison to other specialised areas of international law, such as international humanitarian law (IHL), IHRL often finds itself in a subordinate position. One key factor contributing to this subordinate position is the fact that IHL is not bound by the same territorial and substantive constraints as IHRL. International humanitarian law, also known as the law of armed conflict, governs the conduct of armed conflicts and applies to situations where there is an armed conflict, regardless of the geographical location. This broader applicability allows IHL to address a wide range of issues related to armed conflicts, including the protection of civilians, treatment of prisoners of war, and the prohibition of certain weapons. In contrast, IHRL primarily operates within the boundaries of specific territories or regions, focusing on the protection and promotion of human rights within those areas. This limited geographical scope can sometimes result in IHRL taking a backseat to other areas of international law, including IHL. However, it is important to note that despite its limited geographical scope, IHRL plays One example of how International Humanitarian Law (IHL) is able to effectively deal with the actions of non-state actors that occur across borders is by providing a framework that specifically addresses this issue. By recognising the unique challenges posed by non-state actors, IHL has developed provisions and mechanisms that enable it to regulate and hold accountable these actors for their conduct, even when it occurs outside the territory of a particular state. This ensures that no individual or
are currently experiencing a process of erosion or transformation, as exemplified below. The advancements in technology have played a significant role in the progression of digital human rights. These advancements have not only facilitated the protection and promotion of these rights but have also been influenced by them to some extent. Nevertheless, as demonstrated beneath, the majority of these conventional characteristics of IHRL are presently undergoing erosion or metamorphosis. Such advancements enable the progression of digital human rights and are, concurrently, promoted by them, to some degree.

**Digital Human Rights and Extraterritoriality:** The geographical concentration of International Human Rights Law (IHRL) is undergoing a shift. The European Court of Human Rights (ECtHR) and the European Commission of Human Rights have played a leading role in developing the concept of extraterritorial jurisdiction in specific cases that involve effective control over territories, such as instances of hostile occupation, as well as the exercise of state authority over individuals, such as in the context of foreign detention facilities or the provision of consular services. However, the ECtHR has maintained the view that the extraterritorial application of the European Convention on Human Rights (ECHR) remains exceptional in nature. Furthermore, it has rejected the notion that the mere ability to interfere with the enjoyment of a right confers authority over the right's holder.

Other human rights organizations have adopted a more practical approach towards the application of human rights law beyond national borders. These encompass the Inter-American Tribunal of Human Rights (I/A -T-HR-), which in its 2017 Advisory Judgment on Human Rights and the Environment concentrated on the extent of authority exerted by nations over actions occurring within their borders but nevertheless result in cross-border ecological damage. Likewise, the Human Rights Committee (H.R.C.), in its General Comment 36 of 2018, formulated a jurisdictional criterion encompassing behavior with extraterritorial consequences that has a "immediate and reasonably predictable influence" on the enjoyment of the entitlement to life. Ultimately, in 2021, the Committee on the Rights of the Child adopted "plausible predictability" of consequence as the examination for exercising

---


extraterritorial authority in a climate change lawsuit. (Sacchi v. Argentina, Views of the C.R.C. of Sept. 22, 2021)

When considering the Human Rights Committee (HRC), it becomes evident that the establishment of an operational jurisdictional criterion is closely intertwined with the rise of digital human rights. Specifically, this criterion is crucial in addressing the extraterritorial application of internet surveillance methods, which have become increasingly significant in today's interconnected world. During the comprehensive evaluation of the United States' fourth periodic report in 2014, the esteemed Committee raised valid concerns regarding the extensive coverage in media reports that shed light on the surveillance activities carried out by US security agencies. These activities were not limited to the domestic territory but extended beyond the borders of the United States. The Committee's apprehensions were rooted in the potential implications and consequences of such surveillance practices, which were deemed to have far-reaching effects on various aspects of privacy and security. The activities that were carried out involved the extensive collection of a significant volume of information and metadata, along with the alleged act of eavesdropping on dignitaries from various European nations. In their recommendation, the Committee emphasised the importance of the United States undertaking appropriate actions to safeguard the right to privacy. They specifically called for measures that would guarantee that any potential infringement on this fundamental right adheres strictly to the principles of legality, necessity, and proportionality. It is crucial to note that these principles should be upheld regardless of the individual's citizenship or status, ensuring that everyone's communications are treated with equal respect and protection. According to the Human Rights Committee's report in 2014, it was found that there were several significant issues pertaining to human rights that needed to be addressed. The committee's

Undoubtedly, the practical direction put forth by the Committee's recommendation is a clear manifestation of their profound understanding and recognition of the imperative to broaden the extent of safeguarding offered by the International Covenant on Civil and Political Rights (ICCPR). This imperative arises from the pressing necessity to ensure that the ICCPR remains pertinent and influential as a formidable constraint on state power, particularly in an era characterised by the ever-expanding utilisation of cutting-edge technologies such as internet monitoring.
and unmanned drones. By acknowledging and addressing the challenges posed by these emerging technologies, the Committee's recommendation underscores the significance of adapting and enhancing the protective measures enshrined within the ICCPR to effectively counterbalance the increasing exercise of state authority in contemporary society. During the same US periodic review session, an important topic that was brought up for discussion was the use of drones outside the country. This particular issue shed light on the Committee's recognition of the numerous challenges that arise with the emergence of these advanced technologies. It also emphasised the significance of implementing human rights safeguards to ensure responsible and ethical utilisation of drones. This discussion served as a reminder of the complexities involved in navigating the ethical and legal implications of using drones in international contexts. In an effort to tackle the potential abuse of state authority and safeguard the rights of individuals amidst the rapid advancements in technology, the Committee has taken the initiative to address these pressing issues and emphasise the importance of upholding principles of legality and proportionality. By doing so, the Committee aims to create a framework that promotes accountability, transparency, and fairness, ensuring that the power bestowed upon the state is exercised responsibly and in accordance with the law. This proactive approach seeks to strike a delicate balance between harnessing the benefits of technological progress and safeguarding the fundamental rights and freedoms of individuals, thereby fostering a society that thrives on innovation while upholding the principles of justice and human rights.

**Digital Human Rights and Positive Obligations:** The traditional distinction between civil and political rights, on one hand, and economic, social, and cultural rights, on the other hand, has been gradually eroded in recent decades. Previously, there was a customary interpretation of the International Covenant on Civil and Political Rights (ICCPR) that focused on negative obligations, and an interpretation of the International Covenant on Economic, Social and Cultural Rights (ICESCR) that emphasized positive rights. However, this dichotomy has been significantly diminished. In particular, the European Court of Human Rights (ECtHR) and the Human Rights Committee (HRC) have developed a comprehensive body of legal precedents. For the HRC, this includes its Concluding Observations and General Comments, which impose obligations on governments to take proactive measures to
protect individuals from actions by private entities that impede their enjoyment of rights. These measures can include preventive measures against misconduct, environmental governance, and social assistance initiatives. Given the significant role played by technology companies in enabling the fulfillment of digital human rights, such as freedom of expression, online privacy, and the right to be forgotten, it is not surprising that human rights authorities, including UN Special Rapporteurs for Freedom of Speech and Privacy, have increasingly focused their attention on the regulatory role of governments in relation to technology companies. This reflects the recognition that the actions and policies of these companies have a direct impact on individuals’ ability to exercise their human rights in the digital realm.

After the release of the Ruggie Principles, and Efforts are underway within the United Nations to establish an international legally binding document on business and human rights, building upon the UN Guiding Principles on Business and Human Rights. The current draft document focuses on the obligations of nations to regulate enterprises, including technology firms, to ensure human rights vigilance, enforce legal accountability for human rights violations, provide redress to victims, and engage in global collaboration in implementing the instrument. This framework would apply to technology companies operating on virtual platforms, providing web services, and developing artificial intelligence products.

The Human Rights Committee has thoroughly examined the issue of exporting digital goods, which are produced by private enterprises. This includes the controversial aspect of surveillance technology. The committee has delved into the complexities and implications surrounding the exportation of such goods, taking into account the potential impact on human rights. Through their comprehensive analysis, the committee has sought to shed light on the various dimensions of this issue and provide valuable insights for policymakers and stakeholders involved in regulating the export of digital goods. There has been a growing level of concern expressed by various stakeholders regarding the supply of internet monitoring devices. These devices are provided by corporations that are based in specific countries and are being sold to governments that have a troubling history of human rights violations. This raises significant ethical and moral questions about the potential misuse of these

devices and the implications for individuals' rights and freedoms. One of the key issues that has been highlighted is the lack of legal safeguards and supervisory mechanisms in place when it comes to the export of these monitoring devices. This raises concerns about the potential for abuse and the violation of privacy rights. Without proper oversight and accountability, there is a risk that these devices could be used to target and suppress dissent, curtail freedom of expression, and infringe upon the privacy of individuals. The involvement of corporations based in certain countries adds another layer of complexity to this issue. It raises questions about the responsibility of these companies to ensure that their products are not being used in ways that violate human rights. Additionally, it raises concerns about the potential for these companies to be complicit in enabling human rights abuses by providing these monitoring devices to governments with a history of such violations. The international community has been grappling with these concerns and seeking ways to address them. Efforts have been made to establish international norms and guidelines to regulate the export. In order to ensure that all enterprises, with a specific focus on technology companies, are actively upholding human rights norms during their activities abroad, a comprehensive set of steps has been recommended. These steps aim to promote ethical practices and responsible behaviour, thereby fostering a global business environment that respects and protects the fundamental rights of individuals. By adhering to these guidelines, technology companies can play a crucial role in advancing human rights on a global scale. First and foremost, it is essential for enterprises to conduct thorough human rights due diligence before engaging in any activities abroad. This involves assessing the potential impact of their operations on human rights, identifying any risks or adverse effects, and implementing appropriate measures to mitigate these. The United Nations Special Rapporteur on Freedom of Speech has recently drawn attention to the detrimental effects of spyware applications on political expression. In light of this concern, the Special Rapporteur has advocated for the implementation of temporary restrictions on the export of such applications. This call for action reflects the growing recognition of the potential dangers posed by spyware in curbing individuals' ability to freely express their political views. By emphasising the need for limitations on the export of spyware, the Special Rapporteur aims to safeguard the fundamental right to freedom of speech and protect individuals from potential abuses of these intrusive technologies.
These developments reflect ongoing efforts to address the human rights implications of business activities, including those in the digital sphere, and to establish mechanisms for accountability and safeguarding human rights in the global context.

3.2 TECHNOLOGICAL ADVANCEMENTS

Technological progressions have a pivotal function in moulding the virtual terrain and offer both prospects and hurdles in the execution of virtual regulations to safeguard virtual entitlements. Below are a few illustrations of scientific progressions that have had a noteworthy influence. These technological progressions exhibit the metamorphic capability of digital technologies. Nevertheless, they additionally elevate intricate lawful and moral predicaments that necessitate resolution in the execution of electronic regulations to safeguard electronic entitlements. Balancing innovation and progress with the protection of privacy, security, and individual rights requires proactive and adaptive approaches in the legal and regulatory frameworks.

The swiftly developing digital terrain poses noteworthy obstacles in the execution of digital regulations to safeguard digital entitlements. Several primary obstacles comprise:

Swiftly developing electronic terrain: The electronic terrain is incessantly transforming with novel technologies, platforms, and electronic customs emerging at a swift rate. This energetic milieu renders it arduous for lawful and regulatory structures to stay abreast of the most recent advancements and adjust correspondingly.

Challenge in staying abreast with novel advancements in technology: Fresh advancements, like machine learning, distributed ledger technology, and simulated reality, present innovative lawful and moral predicaments. As these technologies evolve, they may bring unforeseen risks and implications for digital rights. It can be difficult for policymakers and lawmakers to fully understand the complexities and potential impacts of these technologies and develop appropriate regulations in a timely manner.

Restricted capacity to govern nascent technologies: Novel technologies frequently surpass the advancement of rules and benchmarks. This generates a hiatus in the capacity to efficiently govern and safeguard digital entitlements concerning these technologies. The regulatory landscape may struggle to keep up with the pace of innovation, leading to potential vulnerabilities and risks for individuals' digital rights.
Tackling these obstacles necessitates preemptive actions and an adaptable strategy towards governance. Decision-makers and legislators must give precedence to keeping themselves updated about developing technologies, participating in continuous conversations with specialists and concerned parties, and carrying out comprehensive evaluations of probable hazards and advantages. Cooperation among administrations, tech specialists, and community groups is vital to connect the disparity between technological progress and lawful structures. Furthermore, creating systems for ongoing surveillance and assessment of the online environment can aid in recognising new obstacles and advising strategy formation promptly. By adapting to the rapidly evolving digital landscape and ensuring the ability to regulate emerging technologies, digital laws can better protect and uphold digital rights in an ever-changing digital environment.15

4 DISCUSSION AND FINDINGS

Presently, all individuals are cognisant that entry to the worldwide web can result in predicaments connected to the infringement of human entitlements while utilising online mechanisms, owing to unsuitable conduct of individuals functioning within diverse territories, lawful, governmental, and informational customs. As per the scholars’ observation, the emergence of the World Wide Web has not brought forth a fresh set of novel actions - mainly, it duplicates prior patterns. Merely the outcomes of such conduct and the issues linked with its lawful governance have altered16. The nation and community encounter significant duties: to recognise novel entitlements and opportunities for the advancement of customary entitlements. Lawmakers, researchers, and experts in the realm of data and communication technologies are summoned to provide theoretical and satisfactory resolutions to these assignments and concerns.

Any evaluation of the influence of novel technologies on human rights, as Jacopo Coccoli highlights, is exceedingly intricate and necessitates preliminary contemplation of two facets. The initial one is influenced by the developmental duration that divides the accomplishments of technical advancement and their lawful documentation. Modification of both domestic and global lawful regulations to advancements in knowledge and engineering, particularly to electronic technologies, is excessively sluggish and inefficient. The subsequent feature mirrors the inclination of their progress on a global

scale. Considering these factors, it is crucial to establish objectives in the realm of safeguarding human rights: primarily, it is imperative to reexamine traditional human rights in the context of scientific and technological advancement; secondly, novel human rights emerge, which can be characterised as unique - a cohort of electronic rights.\textsuperscript{17}

The process of digitisation accelerates the fusion of limits amid customary sectors of jurisprudence. Data and advancements are currently prevalent in all sectors, they serve as a shared factor and have the potential to establish a cohesive system of regulations. The significance of the limits of legal categories diminishes in the implementation of jurisprudence, which unavoidably impacts the doctrine of jurisprudence. The classification of electronic entitlements is slowly gaining acknowledgement in worldwide, continental, and domestic settings. Occasionally, this occurs during the process of overseeing particular human entitlements, which are commonly denoted as electronic or correspondence entitlements, but at times on a more extensive scale - while ascertaining an exhaustive inventory of such entitlements. Simultaneously, a corresponding classification of entitlements known as cyber entitlements has yet to attain widespread acknowledgement in either legislation or scholarship, taking into account Ukrainian lawful and law enforcement know-how. Apparently, this is dependent on the reality that the predicament of discovering and ascertaining the particular characteristics of essential human entitlements (their essence and execution) in the electronic milieu has emerged comparatively lately and, conceivably, resolving this matter is a concern of the imminent future. Regardless, the objective of today ought to be to comprehend the current concepts concerning electronic entitlements and their rightful owners and meanings, what advantages they aim to safeguard, their interrelation with essential entitlements and liberties (how autonomous they are). In a broad comprehension, electronic entitlements ought to be construed as a continuation of all-encompassing human entitlements to the necessities of a knowledge-oriented community. The writers of this investigation hold the viewpoint that digital entitlements may encompass a vast range of essential entitlements that are executed in a digital milieu and necessitate exploration concerning the characteristics of this milieu. Moreover, essential cyber entitlements are predominantly inferred from data entitlements, but they are not diminished to them.\textsuperscript{18}


\textsuperscript{18} "Tomalty, J. (2017). Is there a human right to Internet access? Philosophy Now, 118, 6-8."
Entrance to the web itself holds no lawful significance, it is crucial as a mechanism of accomplishing other human entitlements and liberties in general - the foundation of all the human's inherent entitlements. The societal structures and methods of human autonomy are manifold and chronologically changeable. Currently, they are becoming increasingly technologically proficient and reliant on technology. The cyberspace (and the necessity for entry to it) is one of the indications of this inclination. Precise communally, traditionally and ethnically established (embracing technologically) methods of practising individual autonomy could feasibly meet the criteria as human entitlements. Confessedly, the practise of nearly all human entitlements remains attainable without the entry to the World Wide Web but is unquestionably less efficient.

The matter of safeguarding human rights while utilising the Internet persists to be exceedingly pertinent in terms of defending human rights. Hence, delegates from one of the most ancient academic and exploration hubs in Spain located at the University of Zaragoza, Professor F. Galindo and Professor J.G. Marco, challenge whether the World Wide Web has the potential to enhance liberty of speech and knowledge without limiting the autonomy of its consumers. Researchers logically observe that the extensive utilisation of data and exploration mechanisms and their automation, on the other hand, assist in reaching diverse data stashed on the web, and hence aid in enhancing liberty. Conversely, it generates predicaments associated with confidentiality, insufficiency of clarity in the utilisation of data and command by consumers. F. Galindo and J.G. Marco aptly observe that search terms combined with associated metadata have the potential to allow nearly anyone to acquire details about the user, such as their likes, routines, and inclinations. Furthermore, certain enquiries might encompass identifiers and quasi-identifiers that enable them to be associated with a specific individual19.

An additional crucial matter emerges from the perspective of both theory and implementation of lawful control – this pertains to the accountability of online middlemen. This predicament is not novel, it has been the focus of numerous investigations, the most captivating of which is the treatise of the University of Liverpool J. Riordan The Responsibility of Web Intermediaries20. The writer endeavours to establish the boundaries of accountability and contemplate them from the perspective of diverse fields of jurisprudence. This research seeks to assist magistrates, professionals,

---
and scholars in suggesting more lucid and uniform regulations overseeing the undertakings of the upcoming cohort of online middlemen, along with controversies linked to their amenities.

The accountability of online middlemen encompasses a vast range of concerns, thereby stimulating the curiosity of the scholarly circle in resolving them. Moreover, the findings of the research indicate that augmenting the accountability of online middlemen and stress on them may unfavourably impact the operations of the commercial realm linked to information. As observed, while determining such accountability, it is constantly crucial to recollect that while creating fitting determinations, vigilance should likewise be practised to guarantee that functional corporate frameworks are not annihilated. J. Riordan justifiably opines that cognisance of knowledge ownership, information security, open internet principles, operational framework, and antitrust regulations are domains where decision-makers and lawmakers must adopt an equitable, commensurate methodology in ascertaining liability. The council of Europe’s committee of ministers has proposed a suggestion regarding the function and obligations of online middlemen. The paper outlines global human rights norms in scenarios where nations limit the operations of online middlemen (such as via censorship and erasure of material or any other actions that could result in constraints on the entitlement to knowledge and expression). Electronic technologies have the potential to surmount bias (such as by broadening entry to fiscal amenities via the growth of cell phone currency) or reinforce it. The second option is frequently linked with the possible capacity of formulas to replicate prejudiced behaviours. Consequently, in the proclamation concerning the manoeuvrable potentialities of algorithmic procedures, the Committee of Ministers of the Council of Europe observes that scientific advancements enable us to deduce quite comprehensive inferences about individuals based on obtainable information, assigning them to specific classifications. This exercise solely strengthens the presently prevailing types of societal, traditional, faith-based, juridical, and financial partition. This enables the allocation of individuals according to their online profiles. Such deeds may have a straight influence on their existence, particularly when an AI system is employed to determine who should mainly qualify for a home loan or medical care. Connectivity safety specialist H. Abelson additionally composes concerning confidentiality concerns. He asserts that

the damage that conferring the sole privilege of entry to data to law enforcement agencies can bring about will be exceedingly grave. Besides the anticipated technical challenges, the quantity of issues linked to overall governance will escalate. In this kind of circumstance, there are no assurances that the values of deference for human rights and the principle of legality would endure.\(^2^2\) Hence, the peril of disseminating classified information is rather elevated. The matter of guaranteeing confidentiality is consistently developing. The community is progressively engrossed in the online realm, and the governing bodies are striving to manage the openly accessible information that is shared on social media to the greatest extent feasible. Without a doubt, such an elevated degree of government oversight weakens the individual's entitlements to express themselves and jeopardises the bedrock of a democratic society.

The manipulation and scrutiny of information that is accessible to the public can have extensive outcomes for the community, and it is especially hazardous for diverse marginalised groups and individuals with dissenting perspectives. It is imperative to establish a collection of fundamental regulations at both the regional and municipal tiers that would enable the surveillance of cutting-edge technologies employed in governmental supervision of inhabitants. Moreover, it is imperative at the countrywide scale to strengthen the fundamental safeguard of individuals against disproportionate government surveillance of online platforms and other openly accessible information. The influence of novel technologies on human rights is also progressively capturing the interest of scholars from diverse fields of jurisprudence. Therefore, electronic technologies have brought apparent modifications to employment legislation. In numerous sectors of the economy, contemporary technologies enable executing a job role beyond the site of employment and workstation, not solely at one's residence (remote office), but additionally in any suitable setting (portable office).

The boss frequently anticipates that a worker will be accessible constantly. In emerging economies, this is considered an advantage and is viewed favourably by labourers who desire to earn additional income and by customers who feel at ease shopping during nighttime hours. However, in industrialised nations, customary principles (such as the entitlement to leisure and seclusion) are dominant. In France, during August of the year 2016, the legislation regarding Employment, enhancement of

social communication, and guaranteeing occupational pathways was sanctioned, wherein one of the segments is referred to as adjustment of employment legislation in the electronic era. Initially, the legislation instituted the entitlement of a worker to power down electronic gadgets (specifically, phone and electronic mail) to abstain from infringing upon their leisure period, time off, and also to honour their personal and domestic existence. Stated differently, French workers possess the entitlement to refrain from responding to their employer's phone calls and electronic messages outside of working hours. And truly, during weekends and holidays, the French are nearly unreachable. France emerged as the pioneer nation to incorporate this entitlement in employment regulations.

As professional demands can no longer fill up the leisure time of workers, there is a hopeful likelihood that a significant fraction of these workers will utilise even greater amounts of time on social media platforms like Facebook, YouTube, or Twitter. Consequently, compensated expert duration has the potential to be substituted with virtual labour, notably on nano-engineering amenities like Amazon Mechanical Turk.

Digitisation may additionally update the realm of ecological legislation. Especially, judicial conflicts concerning the condition of the ecosystem in a specific region would be settled more swiftly if a system were furnished for conveying information on the condition of contamination to the community instantaneously. In regulatory jurisprudence, there are additionally numerous novel occurrences that impact the methodology for executing governmental management. Mechanisms for digital involvement of citizens in governance are being formulated, and methods of enlightening society by governmental organisations are being enhanced. Nonetheless, not only worries are expressed, but specific affirmations that social media, and the World Wide Web in general, present a peril to both democracy and the government itself. The government traditionally endorses synchronisation and intervention systems for the populace, lessening personal interactions of individuals. In the year 2013, the United Nations cautioned that nations jeopardise being excluded from the interaction between individuals. This is what motivates states to proactively access the Internet themselves. State participation in the virtual realm is becoming a crucial element. These procedures have not bypassed Ukraine.

The adjustment of both domestic and global lawful regulations that are intended to manage the realm of knowledge and the most recent advancements is sluggish, and the
present laws are insufficient to appropriately manage the circumstances produced by technical advancements. At the worldwide stage, this issue was resolved by UN decision 2450 (XXIII), which suggests to initiate a multidisciplinary exploration at the domestic and global stages aimed at establishing norms for the safeguarding of human rights and liberties from the possible influence of novel technologies. The decision urges concentrating endeavours on creating an equilibrium between scientific and technological advancement and the cognitive, ethical, artistic, and ethical prosperity of countries. At the echelon of the Council of Europe, the influence of novel technologies on human rights was assessed by all principal powers. The board of ministers and the Legislative Assembly have approved pertinent statements and suggestions, conventions and scholarly exploration are consistently conducted on the laws and customs of diverse Council of Europe nations concerning cyberspace autonomy. The ECtHR additionally contemplates present obstacles to human rights whilst construing the stipulations of the clauses of the ECHR. Matters associated with the gathering and retention of personal information by governmental entities frequently make up a significant portion of the overall quantity of instances concerning the entitlement to honour private existence (Clause 8 of the ECHR). As the European Court of Human Rights has frequently observed in its experience, contemporary technologies for gathering and retention of information can put human rights at risk.

Back in 2008 in the case of S. and Marper vs the United Kingdom, Regarding the perpetual preservation of the candidates' fingerprints, cellular specimens, and genetic profiles in the repository, even after one of them was absolved and the other's case was terminated, the Grand Chamber of the ECtHR emphasised that the utilisation of contemporary scientific techniques in the legal system at any expense was not tolerable. An equilibrium should be established amidst the probable advantages of extensive utilisation of such techniques and the concerns linked with safeguarding confidentiality. Every territory that employs state-of-the-art scientific improvements bears a distinct

obligation to sustain an equitable equilibrium. The tribunal concluded that the absolute and haphazard quality of the authorities’ abilities concerning the preservation of fingerprints, cellular specimens, and genetic information of individuals accused of offences but not found guilty of them, as was the scenario in the mentioned lawsuit, did not achieve an equitable equilibrium between the opposing communal and personal concerns.

Several instances pertain to information gathering via covert interception of messages and, notably, the presence or lack of efficient measures to prevent misuse in this domain. In Szabo and Vissy vs Hungary\(^{27}\) 2016 Regarding Hungarian laws on covert counterterrorism monitoring, the complainants expressed their worry that they might possibly be subjected to such monitoring under the guise of safeguarding public security, with actions of intrusion into their personal life unwarranted and excessive due to the inadequacy of that legislation, notably because it did not include legal oversight over determinations made by the specialised agencies. The European Court of Human Rights observed that the outcome of the struggle against demonstrations of contemporary terrorism is the aspiration of nations to employ cutting-edge technologies for gathering data, like widespread surveillance of communication channels. However, to prevent terrorist acts, the state is obliged to take measures to ensure that the legislation governing the use of such technologies does not allow for the possibility of their abuse. The tribunal determined that under these circumstances, the prerequisite was not satisfied - as per the legislation, monitoring actions had the potential to be enforced on practically any individual in Hungary, and advancements in technology enabled the accumulation of data on a large scale, encompassing individuals who were beyond the purview of the mission. Moreover, the order to apply such measures was issued by the executive authorities and could not be appealed.

In May 2014, the European Court of Justice issued a decision\(^{28}\) Endowing inhabitants of EU nations with the privilege to appeal to any exploration tools with a demand to eliminate specific hyperlinks encompassing confidential data regarding


petitioners. The tribunal highlighted that in case the appeal is reasonable and there are no hindrances to its implementation, the exploration mechanism overseer must be compelled to comply with the appeal. The ruling from the court was unexpected, as it went against the viewpoint of the EU Court of Justice’s Advocate General, who was of the belief that the Google search engine should not be deemed as an organisation that manages private information on the web pages it handles. Remarkably, the Legal Counsel possesses identical credentials as magistrates, and it is his obligation to offer an autonomous and well-founded viewpoint on a specific lawsuit that has reached the European Court of Justice, prior to the judges themselves commencing to scrutinise the assertion on its substance. The viewpoint of the Legal Counsel does not possess the power of a judicial ruling, however predominantly the tribunal considers its suggestions. The litigation concerning the right to be forgotten was a rare occurrence in which the tribunal disregarded the stance of the Advocate General. The verdict rendered by the European Court of Justice was favourably evaluated, it was an actual triumph in the struggle for safeguarding the private information of Europeans. The verdict of the tribunal validated the necessity of transferring the regulations of safeguarding data from the prehistoric digital era to the present-day society, and granted a chance to reinforce and broaden the entitlement of individuals to be erased from the web.

Therefore, concepts regarding the ubiquity of human rights can be seamlessly connected to the impartiality and ubiquity of digital technologies. During the age of computerisation, the core of an individual and their primary necessities are improbable to transform, along with the fundamental principles linked with them. Furthermore, it is the fundamental entitlements of individuals that possess the potential to transform into a cohesive and intentional viewpoint when assessing different technologies. This process entails scrutinising the impact that these innovations have on the liberties, integrity, and respect of human beings. This concept appears highly encouraging, considering the particular perplexity of researchers and professionals when confronted with the obstacles presented by the digital era.

5 CONCLUSION AND SUGGESTIONS

To sum up, the obstacles presented by the opposition from technological corporations in executing digital regulations to safeguard digital entitlements are

substantial. Worries regarding conceivable diminution of earnings, resistance to control and supervision, and their sway on policy formulation and execution might generate hindrances in the establishment of all-inclusive and efficient regulatory structures. Nevertheless, tackling these obstacles is essential to guarantee the safeguarding of virtual entitlements in a swiftly changing virtual terrain.

Equilibrating the concerns of technological enterprises with the wider societal welfare necessitates lucid, comprehensive, and fact-supported policymaking procedures. Participating in significant conversations with every concerned party, such as tech corporations, non-governmental organisations, and specialists, may assist in resolving issues, discovering shared interests, and creating legal structures that safeguard online liberties while encouraging progress and financial advancement.

Furthermore, sturdy regulatory structures, supervision systems, and implementation actions ought to be established to hold tech corporations responsible and guarantee adherence to electronic regulations. Clarity, liability, and communal consciousness are crucial to alleviate the unwarranted sway of technological corporations and emphasise the safeguarding of virtual entitlements.

Through manoeuvring the obstacles presented by the opposition from tech corporations, decision-makers can strive towards enforcing electronic regulations that achieve equilibrium between novelty and the safeguarding of people's digital entitlements. This will aid in cultivating a digital atmosphere that maintains essential entitlements, enables individuals, and advances an equitable and comprehensive digital community.

**CALL TO ACTION FOR INTERNATIONAL COOPERATION**

Confronting the obstacles in executing electronic regulations to safeguard electronic entitlements necessitates worldwide collaboration. Governments, tech firms, societal organisations, and global groups should collaborate in order to surmount the intricacies of the digital realm. An appeal to prompt global collaboration encompasses:

**Cooperation and Conversation:** Encourage transparent and comprehensive communication amidst concerned parties on a global, local, and continental scale. Simplify channels for knowledge exchange, optimal methodologies, and collaborative troubleshooting to tackle the difficulties as a group.
Standardisation of Statutes: Motivate nations to standardise their statutes and rules concerning electronic entitlements to establish uniform and logical structures. Global accords and benchmarks may act as directing ideals to guarantee synchronisation whilst upholding varied lawful conventions and ethnic standards.

Reciprocal Judicial Support: Enhance systems for reciprocal judicial support and knowledge exchange between nations to expedite transnational enquiries and collaboration in instances of digital liberties infringements. Improve synchronisation and optimise procedures to hasten the recognition and indictment of culpable individuals.

Capability Enhancement: Provide assistance for capability-enhancement programmes to improve legal proficiency, technological aptitude, and digital fluency. This will empower nations to establish resilient and efficient structures, tackle evolving obstacles, and guarantee efficient enforcement of electronic regulations.

Cognisance and Instruction: Boost communal cognisance and instruction regarding electronic entitlements, their significance, and methods to safeguard them. Enable people to comprehend their entitlements, champion for their safeguarding, and take knowledgeable decisions in the cyber domain.

Suggestions for Addressing the Challenges: Forward-thinking Regulations: Authorities must forward-thinkingly establish regulations that foresee scientific progress and upcoming obstacles. Promote nimble regulatory structures that can adjust to the swiftly changing digital terrain.

Multi-party Involvement: Engage a broad spectrum of stakeholders, such as tech corporations, non-governmental organisations, higher education institutions, and specialists, in the process of creating policies. Guarantee varied viewpoints are taken into account to formulate all-inclusive and equitable digital regulations.

Moral principles for developing technologies that are new and innovative: Promote the advancement of moral structures and principles for up-and-coming innovations like machine learning, distributed ledger technology, and physiological measurement technologies. This shall aid in tackling worries pertaining to confidentiality, liability, and probable prejudices.

Enhance global coordination and collaboration by means of international treaties, pacts, and collaborative frameworks. Encourage knowledge dissemination, optimal procedure interchange, and partnership regarding transnational concerns.
Autonomous Supervision and Adherence: Create self-governing supervision entities and efficient implementation mechanisms to guarantee conformity with digital regulations. Furnish these entities with sufficient resources, power, and proficiency to efficiently oversee and implement safeguards for digital entitlements. By welcoming global collaboration, implementing preemptive actions, and engaging a variety of participants, the obstacles in executing digital regulations to safeguard digital entitlements can be efficiently tackled. This will aid in constructing a worldwide digital environment that values and maintains the essential liberties of people in the digital era.
REFERENCES


The Author(s), 2023. Published by Cambridge University Press on behalf of the German Law Journal. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.


See e.g., KLAUS SCHWAB, THE FOURTH INDUSTRIAL REVOLUTION 3 (2017). Among the offshoots of the digital revolution one can mention the connectivity revolution, the AI revolution, the big data revolution, the cloud revolution and their fusion with other new technologies, such as blockchain, natural language processing, and biometrics.


See Vasak, supra note 3; see also SAMUEL MOYN, THE LAST UTOPIA: HUMAN RIGHTS IN HISTORY 225 (2010).


See Dror-Shpoliansky & Shany, supra note 7, at 1266–267; see also Tomer Shadmy, Content Traffic Regulation: A Democratic Framework to Address Misinformation, 63 JURIMETRICS 1 (2022).


See e.g., Regulation (EU) 2016/679 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 (General Data Protection Regulation), art. 21, OJ L 119/1 (2016) [hereinafter GDPR].

See Dror-Shpoliansky & Shany, supra note 7.


Cf. Saskatchewan (Human Rights Commission) v. Whatcott, [2013] 1 S.C.R. 467 (Can.), 114 (“hate speech can also distort or limit the robust and free exchange of ideas by its tendency to silence the voice of its target group”).

See e.g., ROBERT H. BLANK, INTERVENTION IN THE BRAIN: POLITICS, POLICY AND ETHICS 80 (2013).


See European Declaration on Digital Rights and Principles, supra note 8, at pmbl. recital 2.

See e.g., Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), June 8, 1977, 1125 U.N.T.S. 609

Advisory Opinion on the Environment and Human Rights of November 15, 2017 (I/A CHR), 102.


See I/A HRC Advisory Opinion (2017), supra note 53.
Sacchi, supra note 55.


See e.g., Simma & Pulkowski, supra note 19, at 511.


See e.g., I/A Advisory Opinion, supra note 53, at 44; H.R.C., General Comment 36, supra note 54, at 26, 31, 62, 64–66,

Hassan v. UK, App. No. 29750/09, para. 102 (Sept. 16, 2014), https://hudoc.echr.coe.int/fre?i=001-146501. Note that the reference to other bodies of law has not been free from controversy and concerns have been raised concerning the expertise of members in IHRL bodies in non-IHRL issues, and about the increased potential for inconsistent decisions across different international bodies. See e.g., Shana Tabak, Ambivalent Enforcement: International Humanitarian Law at Human Rights Tribunals, 37 MICH. J. INT’L L. 661, 707–12 (2016).

See e.g., European Declaration of Digital Rights and Principles, supra note 8, at Ch. 5.


