

TSUL LEGAL REPORT

INTERNATIONAL ELECTRONIC
SCIENTIFIC JOURNAL

VOLUME 6
ISSUE 4
DECEMBER 2025



JOURNAL DOI: 10.51788/tsul.lr.
ISSUE DOI: 10.51788/tsul.lr.6.4.
E-ISSN: 2181-1024



Founder: Tashkent State University of Law



TSUL LEGAL REPORT
T L R

INTERNATIONAL
ELECTRONIC SCIENTIFIC JOURNAL

VOLUME 6
ISSUE 4
DECEMBER 2025

JOURNAL DOI: 10.51788/tsul.lr.
ISSUE DOI: 10.51788/tsul.lr.6.3.

«TSUL Legal Report» international electronic scientific journal was registered by the Press and Information Agency of Uzbekistan on April 21, 2020, with certificate number 1342. The journal is included in the list of journals of the Higher Attestation Commission under the Ministry of Higher Education, Science and Innovations of the Republic of Uzbekistan.

Copyright belongs to Tashkent State University of Law. All rights reserved. Use, distribution and reproduction of materials of the journal are carried out with the permission of the founder.

Publication Officer:

Orifjon Choriev

Editor:

Elyor Mustafaev

Graphic designer:

Umid Sapaev

Editorial office address:

Tashkent, st. Sayilgoh, 35. Index 100047.
Principal Contact

Tel.: (+998 71) 233-66-36

Fax: (+99871) 233-37-48

Website: legalreport.tsul.uz

E-mail: info@legalreport.tsul.uz

Publishing license

№ 174625, 29.11.2023.

E-ISSN: 2181-1024

© 2025. TSUL – Tashkent State University of Law.

EDITOR-IN-CHIEF

B. Khodjaev – Rector of Tashkent State University of Law, Doctor of Law, Professor

DEPUTY EDITOR

Z. Esanova – Deputy Rector for Scientific Affairs and Innovations of Tashkent State University of Law, Doctor of Law, Professor

EXECUTIVE EDITOR

E. Mustafaev – Chief Specialist of the Periodicals Sector of the Publishing Department of Tashkent State University of Law

MEMBERS OF THE EDITORIAL BOARD

N. Koutras – Kurtin Law School, PhD (Australia)

H. Yeung – Associate Professor of Leicester Law School, University of Leicester, (UK)

C. Kelley – Associate Professor of Law School of Arkansas University (USA)

A. Younas – Researcher of the Chinese Academy of Sciences, General Director of Ai Mo Innovation Consultants (China)

Sh. Al-Fatih – Lecturer of the University of Muhammadiyah Malang (Indonesia)

A. Jaelani – Lecturer of Sebelas Maret University (Indonesia)

N. Upadhyay – Associate Professor of the Department of Law and Programs of the Symbiosis Law School (India)

Y. Ogurlu – Rector of Balıkesir University (Turkey)

K. Molodyko – Chief Expert of the Institute of National and Comparative Law Research at the "School of Higher Economics" of the National Research University of Russia, Associate Professor of the Department of International Law (Russia)

N. AllahRakha – Lecturer of the Department of Cyber Law of Tashkent State University of Law, Doctor of Philosophy (PhD) in Law (Pakistan)

N. Rakhmonkulova – Professor of the Department of Private International Law of Tashkent State University of Law, Doctor of Law (Uzbekistan)

A. Tadjibaeva – Associate Professor of the Department of Criminal Procedure Law of Tashkent State University of Law, Candidate of Legal Sciences (Uzbekistan)

R. Urinboev – Professor of the Department of Sociology of Law of Lund University, Doctor of Law (Austria)

M. Kudratov – Doctor of the University of Regensburg (Germany)

Kh. Radjapov – Associate Professor of the Department of Business Law of Tashkent State University of Law, Doctor of Philosophy (PhD) in Law (Uzbekistan)

O. Narziev – Professor of the Department of Private International Law of Tashkent State University of Law, Doctor of Law (Uzbekistan)

Sh. Rahmonov – Head of the Department of International Law and Human Rights of Tashkent State University of Law, Doctor of Law, Professor (Uzbekistan)

CONTENTS

12.00.02 – CONSTITUTIONAL LAW. ADMINISTRATIVE LAW. FINANCE AND CUSTOMS LAW

JAHONOV SHOHRUH SHUHRAT UGLI

Legal analysis of journalistic investigation4

SAYFIDDINOV AQLIDDIN ANVARJON UGLI

The role and powers of local councils in the field of local budget management
in Uzbekistan9

12.00.03 – CIVIL LAW. BUSINESS LAW. FAMILY LAW. INTERNATIONAL PRIVATE LAW

SHERMATOV NURIDDIN AKTAM UGLI

Property and intellectual property rights in additive manufacturing (3D printing):
a sui generis perspective within civil law 18

RAHMATOV AZIZBEK ISKANDAR UGLI

The role of mezzanine capital in financing entrepreneurial activity and its legal
regulation 25

12.00.08 – CRIMINAL LAW. CRIMINAL-EXECUTIVE LAW

OTABOEV BOBUR IBRAT UGLI

Concept and characteristics of terrorism financing 38

12.00.10 – INTERNATIONAL LAW

MUMINOV ASILBEK HUSNIDDINOVICH

International legal regulation of the right to internet access: a new generation
of human rights 48



TSUL LEGAL REPORT

Journal home page: www.legalreport.tsul.uz



Received: 30.10.2025

Accepted: 01.12.2025

Published: 30.12.2025

DOI: 10.51788/tsul.lr.6.4./LGWC1735

INTERNATIONAL LEGAL REGULATION OF THE RIGHT TO INTERNET ACCESS: A NEW GENERATION OF HUMAN RIGHTS

Muminov Asilbek Husniddinovich,

Lecturer of the Department of International Law

and Human Rights,

Tashkent State University of Law

ORCID: 0009-0007-7417-2998

e-mail: asilbekmuminov86@gmail.com

Abstract. In this article, it is thoroughly analyzed how the use of the Internet has acquired the status of a fundamental right within the framework of international law and how this process has been successful in some cases. The study examines such important legal frameworks as regional normative documents on human rights, and statements of the Special Rapporteurs, decisions of the UN Human Rights Council as well as the experience of new states. This study reveals important contradictions through theoretical analysis and practical study of Internet disruptions and access barriers. On the one hand, at least at the theoretical level, there is growing international consensus on the issue of digital rights. However, real practice demonstrates an even more alarming picture: government structures continue to impose restrictions largely unpunished, often relying on vague interpretations of national security, which indicates that international law does not have sufficient force to act as an effective barrier. The study shows that although access to the Internet has not achieved the status of an autonomous human right in compulsory contract law, its functional necessity for the exercise of established rights (freedom of expression, freedom of assembly, and freedom of information) has created what can be called *de facto* directly through the back door.

Keywords: internet access, human rights, international law, digital rights, freedom of expression, UN resolutions, internet shutdowns, digital divide

Introduction

Historians are probably shocked by how rapidly the internet has evolved from a novel concept to one that is almost necessary when they reflect on the start of the twenty-first century. It was basically a specialized tool for military researchers

and academics only thirty years ago. Legal frameworks may not have been able to keep up with this rapid change, which gave rise to some genuinely novel problems for international law.

Currently, more than two-thirds of the world's population, or 5.3 billion people,

are using the global network. Although this indicator seems very impressive, it actually hides serious imbalances behind it. The existing difference in access to digital technologies is not limited to the possibility of connecting. The issue also lies in the level of convenience, quality of use, and the authority of government bodies to terminate network communications at their own discretion in politically unfavorable situations. And most people are actually doing so.

The main question arises: should the use of the Internet be recognized as a fundamental human right in the international legal system? This issue is much deeper than the outward appearance. Certain historical processes, such as the abolition of the slave system, the struggle against dictatorial regimes, and the recognition of the unique value of the individual, laid the foundation for the formation of traditional human rights. They emerged gradually, often as a result of painful events and complex political disputes. However, access to the internet has risen from something that didn't exist in just one generation to a vital necessity.

According to some, the rapid development of the internet prevents it from being recognized as a "true" human right. For most of human history, people have lived without a global network. But this argument overlooks an important nuance: technology itself is not the main issue. The important thing is what opportunities are opening up through this technology. Many well-established human rights – freedom of assembly, freedom of expression, the right to information, and even freedom of economic activity – are realized today mainly through the Internet. Governments that restrict access to the Internet not only deprive people of services, but simultaneously suppress a number of basic freedoms.

To put it mildly, the international legal response proved to be complicated. Online protection of offline rights should

be guaranteed by a number of resolutions adopted by the UN Human Rights Council. On paper, they can be heard clearly. However, since the majority of these tools are optional, chaos results. Although they lack enforcement mechanisms, they serve as a representation of global consensus. However, states frequently still impose Internet restrictions based on public order or national security regulations that are generally recognized by international law (OSCE, 2016, July).

These stresses are methodically taken into account in this study. In what ways did international law try to control access to the internet? What are the modern system's shortcomings? And, above all, where do we go from here? Primary sources such as UN resolutions, reports from Special Rapporteurs (especially the renowned 2011 report by Frank La Roye), regional human rights documents, and both favorable and unfavorable new state practices serve as the foundation for the analysis. Because it touches on a number of conflicting interests, this subject is especially intricate and fascinating from an intellectual standpoint. The speed at which technology is developing is astounding. Although some of your worries are more valid than others, you have good reason to be concerned about state security. Important infrastructure is under the control of powerful private companies. Additionally, some people rely more and more on digital communication in their daily lives. To use international legal mechanisms created for a totally different era in order to balance these conflicting interests? The research is attempting to solve this puzzle.

Methods

This study employs what can be referred to as doctrinal legal analysis with empirical additions, which primarily consists of a close reading of legal texts along with actual data regarding how these texts function or fail in real-world situations. Although the primary methodology is based on the examination of international legal

documents, this research consistently asks what is truly taking place on the ground, in contrast to strictly formalistic approaches.

The material under consideration belongs to several different categories, each of which is selected for certain reasons. Firstly, there are mandatory international treaties - the International Covenant on Civil and Political Rights, as well as regional conventions from Europe, Africa, and America. They are important because they create real obligations, although, as we will see, none of them directly mention the internet. They were compiled decades before the World Wide Web. This creates interesting interpretational difficulties (Finland Makes Internet a Basic Right, 2010).

Secondly, non-binding instruments are, first and foremost, the UN Human Rights Council resolutions. Now international lawyers like to argue about whether “soft law” really matters. Skeptics point out that states often support decisions they do not intend to follow. A fair point. However, these resolutions remain important for several reasons: they indicate developing international consensus, provide meaningful recommendations for mandatory documents, and may eventually become customary law. The main resolutions discussed here cover the period from 2012 to 2024, with special emphasis on Resolution 32/L.20 of 2016 (OSCE, 2016, July). This is important because it clearly condemned deliberate internet access violations – and, notably, several major powers opposed this (United Nations, 2016, July).

Thirdly, the reports of the UN Special Rapporteurs, especially on freedom of expression. Frank La Rowe’s 2011 report (A/HRC/17/27) was truly revolutionary – for the first time, an official UN representative officially stated that disconnecting internet access violates international human rights law (United Nations, 2011, June). Subsequent speakers built on this foundation, albeit with varying degrees of courage. These reports do not create a

mandatory right, but they carry significant interpretative power.

Some limitations must now be acknowledged. First of all, technology always advances more quickly than the law. It is inevitable that new problems will surface by the time this study is published. Second, there are differences in how transparent the state is about restrictions. While some governments covertly put pressure on telecom companies and deny everything, others publicly defend disconnections. As a result, there are data gaps that no methodology can completely fill. Thirdly, the emphasis is primarily on the international level, not on the domestic level – monitoring the implementation and compliance with requirements at the national level receives less attention than deserved. But even with these limitations, the basic patterns become sufficiently clear.

Results

The story of how internet access became a human rights problem is essentially a story of legal interpretation and adaptation. None of the major human rights treaties mention the internet – they could not do it as indicated when they were made. The Universal Declaration of Human Rights dates back to 1948. ICCPR until 1966. The Internet, as we know it, did not exist. Nevertheless, these tools were somehow stretched out, quite creatively to encompass digital rights.

Article 19 of the ICCPR provides the basis. It guarantees freedom of opinion and expression “through any mass media” and “regardless of borders” (Banihashemi, 2023). This phrase “any media outlet” has done impressive work over decades. The UN Human Rights Committee in its General Comment No. 34 confirmed that this protection applies to all forms of electronic and online expression (Finland Makes Internet a Basic Right, 210). Not exactly amazing – it would be strange if fundamental rights somehow jumped over the internet. But, nevertheless, the clear confirmation had significance.

However, Frank LaRue's 2011 report went even further. He did not just say that the internet is covered by existing rights. He argued – and this was more controversial – that effectively disconnecting someone's internet access violates Article 19. Regardless of the justification (United Nations, 2011, June). It was bold. The traditional interpretation of Article 19 focused on preventing censorship without requiring states to grant access. La Rowe refuted this: he argued that the internet had become such a central element of freedom of expression that denial of access was itself a form of censorship (Media Defence, n.d.).

The UN Human Rights Council gradually adopted this view. The 20/8 resolution of 2012 was the first to clearly state that online rights are equal to offline rights. A simple principle, profound consequences. If you have offline freedom of expression, you have online freedom of expression. If you have rights to privacy, assembly, and information offline, it's the same online. Resolution 32/L.20 in 2016 went further, particularly condemning measures that "deliberately obstruct or disrupt access to information on the Internet" (OSCE, 2016, July).

But here it becomes politically interesting. The 2016 resolution had over 70 co-sponsors – an impressive number. Nevertheless, several large states opposed this: China, Russia, Saudi Arabia, and others (United Nations, 2016, June). Their objection was not superficial: they argued that the resolution violates the state's sovereignty over communication infrastructure. National security, they said. Public order. Traditional arguments that international law has historically accepted may be too numerous.

By 2021, the Council has instructed to conduct comprehensive research on internet disconnection issues (Resolution 47/16). As a result of the 2022 report, 931 disconnections were documented in 74 countries between 2016 and 2021 (OpenGlobalRights, 2023, July). This

is a surprising number when you think about it. And that's probably not enough – governments that shut down the internet don't always say it openly. About half of these outages occurred during protests or elections. A coincidence? The report diplomatically stated that it might not.

When can governments legally restrict internet access? International law provides the answer, at least theoretically. It is called a three-part test based on Article 19 (3) of the ICCPR. Any restriction must: (1) be provided for by law, (2) pursue a legitimate goal specified in the Covenant, and (3) be necessary and proportional to the achievement of this goal (Right to access the Internet, 2011, May). That sounds reasonable. The devil, as always, lives in the details.

"It's stipulated by law" seems obvious – there must be legal grounds for restrictions. But what is considered an adequate legal basis? In many countries, there are unclear laws on national security or public order that can justify almost everything. A law may exist technically, but if it is so extensive that it provides unlimited freedom of choice, does it truly satisfy this need? The Human Rights Committee says no, such laws are too broad. States often ignore this inconvenient detail.

"Legal goals" include such things as national security, public order, protecting the health or morality of the population, and protecting the rights of others. Sufficiently just – these are real state interests. The problem is how states address them. Freezing during protests? Public order. Blocking social media during elections? National security. What is the throttling capacity in resistive regions? To protect public morality, somehow. Legal goals are real, but they have become comprehensive justifications that are rarely considered with sufficient skepticism.

The "necessary and proportional" requirement should be the true teeth of this test. The Human Rights Committee clearly indicated that restrictions should be

the least intrusive and should be adapted to the specific threat. Common internet disconnections practically never comply with this standard. If you're concerned about specific illegal content, block that content – don't turn off the entire internet for everyone. If you're worried about coordinating violence, focus on specific communications, not excluding all digital connections.

This point is particularly noticeable in the UNHRC report on disconnections in 2022. General disconnections, he concludes, "rarely, if ever" meet the requirements of necessity and proportionality. Think about what it actually means to be completely disabled. This isn't just blocking access to potentially problematic content. This will disable emergency services. Interruption of medical communication. Prevention of enterprise operations. Stopping learning. Isolation of vulnerable population groups. Is all this to eliminate what is usually considered a specific security threat? The analysis of proportionality failed impressively.

Nevertheless, despite all the regulatory developments, their implementation remains weak. States justify closing the case with unclear legal provisions. They claim national security without demonstrating real threats. They refuse to speak openly about who ordered the interruptions and why. And they pressure telecommunications companies to impose restrictions without official orders, creating a reliable negative. The gap between legal norms and real practice is enormous and is constantly growing. Soft legislation can establish norms, but cannot compel them to be enforced. This is the main problem.

Several nations have taken the risk of formally recognizing internet access as a right, despite the fact that international frameworks are still not entirely clear. Their methods diverge greatly, exposing divergent philosophical perspectives on the meaning of such recognition and the responsibilities that go along with it.

In 2010, Finland took the lead by making broadband connections a legal right (Miller, 2021, October). This wasn't merely symbolic; it gave communication operators actual obligations to connect all permanent residential buildings and businesses at a minimum speed of 1 Mbit/s. Finland committed to reaching a nationwide speed of 100 Mbps by 2015. This is true, quantifiable, and doable. This is the appearance of a genuine confession.

Even earlier, in 2000, Estonia backed significant infrastructure investments through the Tiger Leap program, establishing internet access as a human right (European Parliament, 2021, May). Because it connected digital rights to the state's larger development strategy, the Estonian approach is especially intriguing. They constructed infrastructure to give the right significance rather than merely declaring it. Without a way to put them into practice, rights are just nice words.

France took a different route. In 2009, their Constitutional Council decided that internet access is a part of the freedom of expression and communication that is guaranteed by the constitution (European Parliament, 2021, May). Legislation that would automatically block internet access for copyright violations was at issue in this case. The council responded that without a court hearing, it is impossible to deny someone a basic form of self-expression. By restricting the state's power to refuse access rather than mandating that it grant it, it was defending rights through negativity rather than positivity.

Article 5A, which guarantees the right to engage in the information society and requires the state to provide access to electronic information, was added to Greece's 2001 constitution amendments (European Parliament, 2021, May). This is about digital participation in general, not just internet access. It is up for debate whether it strengthens obligations or just sounds more thorough without adding much substance.

International law interprets these domestic occurrences differently. They demonstrate the political viability and possibility of formal recognition. They offer examples of what recognition might actually look like. Additionally, by illustrating state practice, they aid in the formation of customary international law. They also highlight fragmentation, though, as there is no single strategy or consensus on what is truly needed to acknowledge internet access as a right (United Nations, 2023, October).

Perhaps most importantly, official recognition does not guarantee protection. Countries with constitutional or legal protection usually maintain high rates of Internet access and face significant legal barriers to imposing restrictions – which is good. However, even in these countries, the gap between *de jure* recognition and *de facto* common use remains significant. Rural areas lag behind cities. Low-income households cannot afford to buy services even if they have infrastructure. Recognition is important, but it is not enough if it is not properly implemented and insufficiently invested.

The 2030 Agenda for Sustainable Development is approaching internet access from a different perspective than human rights frameworks, and the difference is becoming apparent. Instead of asking “is this right?” he asks “what development goals require digital connectivity?”. It turns out, the answer is most of them.

Target 9.c clearly calls for significantly increasing access to ICT and striving for universal, accessible internet in the least developed countries (Access Now, 2023, January). The language is somewhat hedged – “striving for” rather than “providing,” but the goal acknowledges something important: digital communication has become a fundamental infrastructure comparable to transport, energy, and water. Without it, it is impossible to build the economy of the 21st century.

Connections with other SDGs are extensive and are becoming increasingly evident. Quality education (SDG 4)? Online learning platforms are now necessary, as COVID-19 has proven to be painful. Economic growth and decent work (SDG 8)? Digital commerce and remote work are entirely dependent on the connection. Reducing inequality (SDG 10)? The numerical gap exacerbates every other form of inequality (UNCTAD, 2020). When the pandemic began, those without reliable internet access faced serious difficulties in education, healthcare, employment, and basic social participation (Floridi, 2021).

Nevertheless, progress towards the target date of 2020 (which has obviously already passed) remains inadequate. About 2.7 billion people worldwide still lack access to the internet (OHCHR, 2022, June). This is approximately one-third of humanity. The digital divide is also unevenly distributed – Africa south of the Sahara and parts of South Asia face the largest gaps. This is not just about infrastructure, but also about a systemic deficiency that strengthens existing patterns of global inequality.

Within countries, certain groups face disproportionate barriers. Women, rural populations, people with disabilities, and lower socio-economic groups consistently have lower access rates (OHCHR, 2022, June). This is important because as more and more important services – public services, banking, healthcare, education – go online, those who don’t have access are increasingly being pushed out of civil and economic life. Digital exclusion becomes a social exclusion.

Discussion

Despite the regulatory and legal development, important practical and conceptual problems persist. The most obvious problem is that there is no mandatory international agreement that directly recognizes Internet access as an autonomous human right. Everything is based on the interpretation of existing documents, supplemented by soft

legislative resolutions. This creates uncertainty regarding the specific scope of state obligations and leaves immense freedom of action in national enforcement.

The phenomenon of disconnecting the internet illustrates how weak law enforcement is in reality. Despite international condemnation, documented power outages increased between 2016 and 2021. Governments have also become more sophisticated – complete power outages are becoming increasingly rare, replaced by bandwidth throttling and selective application blocking. They are more difficult to detect and easier to justify as “technical problem” than deliberate limitations. States rarely face significant consequences for violations. UN resolutions expressing concern are good, but they change behavior little, especially in authoritarian contexts (Domaradzki et.al., 2019).

Developing technologies represent problems that current frameworks cannot adequately solve. Take, for example, network neutrality – should internet providers allow discrimination between different types of traffic? International human rights law does not actually state this. Or algorithmic content moderation – when private platforms use AI to filter content, they engage in censorship that should be regulated by freedom of expression principles? It’s unclear. What about the responsibilities of internet providers and technological platforms in general? These are fundamentally private entities, but they control critical infrastructure and make decisions affecting the rights of millions of people (Sander, 2016, November).

There are unique challenges because internet infrastructure is concentrated among a few private companies. Because these businesses operate in multiple jurisdictions, regulatory oversight is challenging. They have conflicting obligations because they are subject to various legal requirements in various

nations. Additionally, they have a great deal of control over access and speech, which states used to have but frequently do not. How should international law handle this? This multilateral setting is not well suited to the current framework created for “state-state” relations and “state-person” rights.

The most basic is probably that technology advances more quickly than the law can keep up. New communication technologies, quantum computing, algorithmic decision-making, and artificial intelligence all bring up issues that haven’t been developed to be solved in the current circles. One attempt to address these new issues is the global digital agreement that the UN Secretary-General has proposed (Floridi, 2021). It’s unclear if this will actually occur. In addition to updating the legislation to reflect modern technology, the task also entails developing adaptable frameworks that can take into account unimaginable future advancements. Yes, this is a complicated issue.

Conclusion

In the context of today’s digital transformation, the right to access the Internet is one of the inalienable human rights. This right is also enshrined in UN resolutions and a number of regional documents. But today, in the context of digital transformation, there are a number of gaps in the protection of human rights.

These important documents include resolutions adopted by the UN Human Rights Council requiring online protection of offline rights. However, there are not enough documents of this recommendatory nature, since we can see aspects of violation of the right to access the Internet around the world in several cases. Due to the absence of mandatory norms in international law, states continue to restrict access to the Internet for the purposes of public order and national security.

There are significant differences between the approaches used in different countries and regions, and successes are noted in some areas. Although proclaiming

progress in many places is more difficult than implementing it in practice, European countries usually stand ahead of other countries in the formal recognition of rights. This situation indicates the complexity of forming common norms for all countries, since each state has its own legal system and level of development.

Of particular importance is the fact that the formal recognition of rights largely depends on the amount of funds spent on infrastructure development, simplified regulatory rules, and the readiness of judicial bodies to prevent the use of excessive force by the state.

Several priority areas have been identified to strengthen defense at the international level. First of all, countries should create a binding international treaty that clearly defines the limits of permissible restrictions and recognizes the use of the Internet as a necessary part of the realization of human rights. This increases efficiency and reduces current uncertainty. Secondly, in order to eliminate the gap in access to digital technologies, developing countries need not only to adopt statements, but also to allocate resources for infrastructure development, facilitation measures, and professional development. Thirdly, emerging technologies require a flexible regulatory framework regarding platform responsibilities, algorithm control, and

personal data protection. Old strategies based on the threats and technological advances of the 20th century are no longer sufficient.

Creating stronger performance mechanisms is probably the most important task of the international team. The gap between theoretical standards and practical public policy can be reduced by not supporting arbitrarily imposed restrictions, improving monitoring systems, and holding violators accountable. Although non-binding rules have led us much further, their weaknesses are becoming increasingly apparent.

Access to the Internet serves as a clear example of how human rights principles are adapting to technological changes. Instead of developing entirely new and complex legal categories, the international community chose the path of logical development of existing systems, taking into account the specifics of digital communication. As technology advances, this flexible but ethical approach becomes increasingly important.

At a time when digitalization processes are accelerating, one of the main goals of international law in the 21st century is to ensure the continued effective protection of human rights in societies that are increasingly transitioning to digital form. Time will tell if we can successfully solve this complex task.

REFERENCES

1. Australian Human Rights Commission. (n.d.). *A right to access the internet*. <https://humanrights.gov.au/our-work/8-right-access-internet>
2. Access Now. (2023, January). *More than 3.5 billion left in the dark: Why we're still fighting to reach U.N. targets for internet access*. <https://www.accessnow.org/internet-access/>
3. Banihashemi, P. (2023). International law and the right to global internet access: Exploring internet access as a human right through the lens of Iran's Women-Life-Freedom movement. *Chicago Journal of International Law*, 24(1), 53–98.

4. Cali, B. (2020). The case for the right to meaningful access to the internet as a human right in international law. In *The Cambridge handbook of new human rights* (pp. 263–280). Cambridge University Press.
5. Domaradzki, S., Khvostova, M., & Pupovac, D. (2019). Karel Vasak's generations of rights and the contemporary human rights discourse. *Human Rights Review*, 20(4), 423–443. <https://doi.org/10.1007/s12142-019-00565-x>
6. European Parliament. (2021, May). *Internet access as a fundamental right* (Briefing PE 696.170). [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696170/EPRS_STU\(2021\)696170_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696170/EPRS_STU(2021)696170_EN.pdf)
7. Floridi, L. (2021). A just digital framework to ensure equitable achievement of the Sustainable Development Goals. *Nature Communications*, 12, Article 6345. <https://doi.org/10.1038/s41467-021-26619-6>
8. *Finland makes internet a 'basic right'*. (2010). PBS NewsHour. <https://www.pbs.org/newshour/world/finland-broadband-law>
9. Kaye, D. (2017, June 1). *Why internet access is a human right*. Carnegie Endowment for International Peace. <https://carnegieendowment.org/2017/06/01/why-internet-access-is-human-right-pub-70151>
10. La Rue, F. (2011, May 16). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/17/27)*. United Nations Human Rights Council. <https://digitallibrary.un.org/record/706331>
11. Media Defence. (n.d.). *The right to freedom of expression under international law*. <https://www.mediadefence.org/ereader/publications/modules-on-litigating-freedom-of-expression-and-digital-rights-in-south-and-southeast-asia/module-1-key-principles-of-international-law-and-freedom-of-expression/the-right-to-freedom-of-expression-under-international-law/>
12. Miller, L. (2021, October). *The human right to internet access*. Voices of Promise. <https://www.promisehumanrights.blog/blog/2021/10/the-human-right-to-internet-access>
13. OSCE. (2016, July). *UN Human Rights Council resolution on protection of human rights on the internet a milestone for free speech, says OSCE representative*. <https://www.osce.org/fom/250656>
14. Office of the High Commissioner for Human Rights. (2011, June 3). *Internet should remain as open as possible – UN expert on freedom of expression*. <https://www.ohchr.org/en/press-releases/2011/06/internet-should-remain-open-possible-un-expert-freedom-expression>
15. Office of the High Commissioner for Human Rights. (n.d.). *International standards*. <https://www.ohchr.org/en/issues/freedomofopinion/pages/standards.aspx>
16. Office of the High Commissioner for Human Rights. (2022, June). *Internet shutdowns: UN report details 'dramatic' impact on people's lives and human rights*. <https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human>
17. Office of the High Commissioner for Human Rights. (2022, June). *Switching off the internet causes incalculable damage: UN report*. <https://www.ohchr.org/en/stories/2022/06/switching-internet-causes-incalculable-damage-un-report>
18. OpenGlobalRights. (2023, July). *Weaponizing internet shutdowns to evade accountability for rights violations*. <https://www.openglobalrights.org/weaponizing-internet-shutdowns-evade-accountability-rights-violations/>
19. Office of the High Commissioner for Human Rights. (2022, August). *Activists: Internet shutdowns violate human rights*. <https://www.ohchr.org/en/stories/2022/08/activists-internet-shutdowns-violate-human-rights>

20. *Right to access the internet: The countries and the laws that proclaim it.* (2011, May). Diplo. <https://www.diplomacy.edu/blog/right-to-access-the-internet-countries-and-laws-proclaim-it/>
21. Sander, T. (2016, November). *The internet as a human right.* Brookings Institution. <https://www.brookings.edu/articles/the-internet-as-a-human-right/>
22. Stephanie, B. P. (2011). *UN declares internet access a human right – did it really?* Diplo. <https://www.diplomacy.edu/blog/un-declares-internet-access-human-right-did-it-really/>
23. Article 19. (2021, July). *Human Rights Council adopts resolution on human rights on the internet.* <https://www.article19.org/resources/un-human-rights-council-adopts-resolution-on-human-rights-on-the-internet/>
24. United Nations Human Rights Council. (2016, June). *The promotion, protection and enjoyment of human rights on the internet: Draft resolution (A/HRC/32/L.20).* <https://digitallibrary.un.org/record/845728>
25. United Nations Human Rights Council. (2016, July). *The promotion, protection and enjoyment of human rights on the internet (Resolution A/HRC/RES/32/13).* <https://www.refworld.org/docid/57e916464.html>
26. Article 19. (2016, July). *Significant resolution reaffirming human rights online adopted.* <https://www.article19.org/resources/unhrc-significant-resolution-reaffirming-human-rights-online-adopted/>
27. United Nations Human Rights Council. (2016, June). *Resolution on the promotion, protection and enjoyment of human rights on the internet (A/HRC/32/L.20).* <https://wilmap.stanford.edu/entries/resolution-promotion-protection-and-enjoyment-human-rights-internet-ahrc32l20>
28. United Nations. (2011, June 8). *United Nations: Warning against internet restrictions issued.* Library of Congress. <https://www.loc.gov/item/global-legal-monitor/2011-06-08/united-nations-warning-against-internet-restrictions-issued>
29. United Nations. (2023, October). *Wired for good: Digital connectivity for a sustainable future.* <https://unsdg.un.org/latest/stories/wired-good-digital-connectivity-sustainable-future>
30. UNCTAD. (2020). *SDG Goal 9.c - Access to ICT.* https://stats.unctad.org/Dgff2016/prosperity/goal9/target_9_c.html
31. World Economic Forum. (2023, March). *Why we can't meet the SDGs without ending the digital divide.* <https://www.weforum.org/stories/2023/03/digital-divide-sdgs-progress>



TSUL LEGAL REPORT

INTERNATIONAL ELECTRONIC
SCIENTIFIC JOURNAL

VOLUME 6
ISSUE 4
DECEMBER 2025