The New International Triangle: Human Rights-Digitalization-Security[1]

Associate professor **Cristina Elena POPA TACHE**[2]

Abstract

Communications and new technology law is the academic endeavor through which legal professionals support education and prepare new generations for the technological future. They will carry forward this experience in economic development, especially in international investments that use technologies in a majority proportion. Today there is no business that does not use the Internet or technological products and international investment law is already creating a ramification in terms of rights and obligations. Will we be dealing with reforms of specific principles and standards? Will the narrow framework of monodisciplinarity be overcome in favour of creation and transdisciplinarity as tools for regulating all derivative aspects? Will the influence of strategic and technological developments on the meaning and interpretation of international law itself be observed? The arguments and conclusions of this paper are meant to emphasize the importance of understanding reality, going through the appropriate meta-analysis filtered through the ethos of the researcher. For the elaboration of this article, the method of specific scientific introspection correlated with the transdisciplinary type method based on primary and secondary sources were used.

Keywords*: international investment, society, transition, digitalisation, international law, transdisciplinarity.*

JEL Classification: F50, K33, O30

1. Introduction

The new International Triangle can be brought together into one idea by recognising the interdependence and mutual influences between human rights, digitisation and security in the digital world, particularly in economic development. These three components are closely interlinked and have a significant impact on the way people live, work and interact in modern society. The keystone of this equal-sided geometry is balanced so that we protect and promote human rights, while ensuring that digitisation and security are used in a responsible and transparent way, with our focus on technological transformation in the conduct of international investment.

Constitutional limits and protections should guide government policy at all levels because all of these limits on government power and all of the protections for

[1] This article is a contribution to the International Conference „Rights and Security", organized by New Bulgarian University in April 27–28, 2023, dedicated to the 75th anniversary of the adoption of the United Nations Universal Declaration of Human Rights and the 20th anniversary of the establishment of the Department of National and International Security and the Diplomatic Institute to the Ministry of Foreign Affairs.

[2] Cristina Elena Popa Tache - associate professor in International Law at the Faculty of Psychology, Behavioral and Legal Sciences of the „Andrei Saguna" University of Constanta, Romania; active researcher at the International Center for Transdisciplinary Research (CIRET) Paris and Co-Chair for European Society of International Law, IG International Business and Human Rights, cristinapopatache@gmail.com, ORCID: https://orcid.org/0000-0003-1508-7658.

individual rights contained in the federal and state constitutions must inform and apply to all government policy regarding communications and technology. They do not cease to apply when practices or conduct relate to digital technology or occur online, because one principle is that the legal rules applicable online are, or should be, identical to the rules applied offline. On the one hand, digital metamorphoses offer many opportunities for economic growth, connecting people around the world, building a sense of community, creating markets and facilitating inclusion, such as better access to education, health and other public services. On the other hand, the same benefits bring exposure of people to new risks, such as security threats, breaches of privacy and restrictions on freedom of expression[3]. Recently, a proposal for comprehensive constitutional changes has been launched in the literature. We know that constitutional provisions are difficult to amend because they involve a laborious process. *However, digital technologies are deeply intertwined with constitutionalism. They are not only a sum of tangible and intangible architecture, but also provide infrastructure for the exercise of freedoms and powers. Internet governance is moving towards fragmentation, polarisation and hybridisation. These trends are not just about the governance of technical infrastructure. It is the beginning of reshaping the architecture of freedom and power in the digital environment, giving impetus to a new role for constitutionalism in the digital age. The key question, therefore, is how far does the evolution of Internet governance lead towards a new constitutional paradigm in the digital age?*[4]

After all, at the centre of the triangle of equal sides: digitisation, human rights and security will be those reforms of constitutional models that protect rights and limits, or rather balance, powers on a global scale. Giovanni De Gregorio and Roxana Radu have shown that these changes demonstrate that constitutional issues are increasingly being considered beyond the state and therefore require public policy approaches that recognise political, technological and economic interests. Attempts to fragment the Internet, a shift in its technical governance towards the integration of standards prone to centralised control and enforcement, could undermine the multilayered protection of rights that derive from international, supranational and national constitutional law. The often-discussed polarization is visible to the naked eye from every corner: the American and Chinese technospheres extend beyond standard-setting processes into the dynamics of global governance, whether for international convention-making or for normative efforts. Ultimately, the hybridization of Internet governance is achieved through international and the continued blurring of the private-private order in the exercise of public interest functions in both democratic and authoritarian systems. When tech giants and digital platforms exercise unlimited power, at stake is the fullness of individual and collective rights and freedoms guaranteed by constitutionalism.[5]

At European level, the most relevant source for principles is: European Declaration on Digital Rights and Principles for the Digital Decade 2023/C 23/01/PUB/

---

[3] OECD, *Rights in the digital age: Challenges and ways forward*, OECD Digital Economy Papers, No. 347, OECD Publishing, Paris, 2022, https://doi.org/10.1787/deb707a8-en, p. 6.

[4] Giovanni De Gregorio, Roxana Radu, *Digital constitutionalism in the new era of Internet governance*, International Journal of Law and Information Technology, Volume 30, Issue 1, Spring 2022, pp. 68–87, https://doi.org/10.1093/ijlit/eaac004.

[5] See for details Giovanni de Gregorio, Roxana Radu, *Digital constitutionalism in the new era of Internet governance*, International Journal of Law and Information Technology, Volume 30, Issue 1, Spring 2022, pp. 68–87, https://doi.org/10.1093/ijlit/eaac004.

2023/89. It is increasingly argued that a just digital transition means that 'human rights and human control over the machine must remain fundamental values'[6]. The European Declaration on Digital Rights and Principles for the Digital Decade states that the European way of digital transformation puts people at the centre and is underpinned by European values and EU fundamental rights, reaffirming universal human rights and benefiting all individuals, businesses and society as a whole. At the same time, the first principle presented in the Declaration is that of digital transformation centered on people[7].

Human rights are enshrined in various international treaties, such as the Universal Declaration of Human Rights, and are designed to protect individuals from discrimination, injustice, and abuse. As technology advances, machines are becoming more powerful and are able to perform tasks that were once only possible for humans. This creates new opportunities, but also raises important questions about how we ensure that these machines are used in ways that respect and uphold human rights. One of the key ways in which human rights and human control over machines must remain fundamental values is through the design and economic development of thought technology.

2. Some observations and strategies to ensure a balance between human rights, digitisation and security, and to identify sustainable solutions to current and future problems

Starting from the date of publication of the Declaration in the Official Journal of the EU on 23.01.2023, it is understood that any document must be interpreted based on the set of principles and rights in the Declaration. According to the right of freedom of choice in interactions with algorithms and artificial intelligence systems, the Declaration states that 'Artificial intelligence should serve as a tool for people, with the ultimate goal of enhancing their well-being'. We can deduce that tools are by definition controlled by people, they are tools or devices suitable for the execution of a certain operation. The declaration includes a special chapter on security, safety and capability. This is Chapter 5 where the commitments made by EU Member States are to protect 'the interests of individuals, businesses and public institutions against cyber security risks and cybercrime, including data breaches and identity theft or identity manipulation'[8] and 'to combat and hold accountable those within the EU who seeks to undermine online security and the integrity of the digital environment or who promote violence and hatred through digital means'.

In the first instance, the digital environment is essential, first and foremost in connecting with its consumers. Consumers' digital engagement takes place in a variety

[6] See European Economic and Social Committee, *Digital transition must be fair: human rights and human control over the machine must remain fundamental values*, available online here: https://www.eesc.europa.eu/ro/news-media/news/tranzitia-digitala-trebuie-sa-fie-echitabila-drepturile-omului-si-controlul-uman-asupra-masinii-trebuie-sa-ramana-valori, accessed on 6.02.2023.

[7] 'People are at the centre of the digital transformation in the European Union. The role of technology should be to serve and benefit all people living in the EU and enable them to pursue their aspirations with full respect for their security and fundamental rights.'

[8] Chapter 5(b) of the Declaration states that 'This includes the imposition of cyber security requirements for connected products placed on the single market'.

of ways, from visiting and browsing a digital service provider's website, to interacting, often critically, with that provider (provider of various digital services) via social networks or clicking on company advertisements[9]. From consumer rights to human rights, the security aspects we observe remain the same, they are the constant in this equation, which underlines the obvious convergence of consumer protection and human rights within EU law, observed by most theorists in recent years. Through this merger, there is a two-way consolidation: from fundamental rights (and other human rights) to consumer protection, and vice versa, especially in the digital sector. The theory has seen an examination of the conceptualisation of consumer protection as a human right and the specific influences[10]. It is worth noting how consumer digital engagement is best examined through a lens of personal and cultural value safety but also through critical research on international marketing and business, from the perspective of the societal cultural value/personal cultural value relationship[11]. Following this line of thought, we enter into the regional analysis of this issue, recalling the changes that have occurred at the level of the European Union.

The EU's Digital Services Act (DSA) brought the latest adaptations marked by some specific obligations. The political agreement on the DSA[12] was reached on 23 April 2022 between the European Parliament and EU Member States, and the final text of the DSA was published on 27 October 2022, with the DSA entering into force in November 2022, with the provisions applying mainly from 17 February 2024 (Article 93)[13]. The accelerating digitisation of society and the economy has found some ground for non-regulation, which has sometimes led to unfair conditions for both investors or providers of these services and a dramatic reduction in consumer choice.

In the age of big data, it is essential that individuals have control over their personal data and can make informed decisions about how it is used. In terms of human control and responsibility, as technology becomes more autonomous, it may become increasingly difficult to assign responsibility for its actions. This can create a risk of harm to people, as it may not be clear who is responsible for any negative consequences that occur.

We recall in this context that the Guide to Human Rights for Internet Users[14] focuses on the following fundamental human rights and freedoms with reference to the

---

[9] See KumarViswanathan, Bhaskaran Vikram, Mirchandani Rohan and Shah Milap, *Creating a measurable social media marketing strategy: Increasing the value and ROI of intangibles and tangibles for hokey* pokey in Marketing Science, 32(2), 2013, pp. 194–212. See also Lamberton Cait, Stephen T. Andrew, *A thematic exploration of digital, social media, and mobile marketing: Research evolution from 2000 to 2015 and an agenda for future inquiry* in Journal of Marketing, 80(6), 2016, pp. 146–172.

[10] Benöhr, Iris, *The Evolution of Consumer Protection and Human Rights*, EU Consumer Law and Human Rights, Oxford Studies in European Law (Oxford, 2013; online edn, Oxford Academic, 16 Apr. 2014), https://doi.org/10.1093/acprof:oso/9780199651979.003.0003, accessed 5 Feb. 2023.

[11] Yuliani Suseno, Doan T. Nguyen, *Culture is in the eye of the beholder: using metaphoric representations of cultural values to enhance consumer digital engagement,* Journal of Strategic Marketing (online), 2021, DOI: 10.1080/0965254 × .2021.1902373.

[12] Hereafter, the Digital Services Act will be used in the text of this article using the acronym DSA.

[13] See Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[14] Recommendation CM/Rec (2014)6 of the Committee of Ministers to member states on the Human Rights Guidelines for Internet Users and Explanatory Memorandum adopted by the Committee of Ministers on 16 April 2014.

Internet: 1) access and non-discrimination; 2) freedom of expression and information; 3) freedom of assembly, association and participation; 4) protection of privacy and personal data; 5) education and literacy; 6) protection of children and young people; and 7) the right to an effective remedy for invoking fundamental human rights and freedoms[15].

Looked at differently, digitisation has a significant impact on human rights and the protection of personal data, and has brought significant benefits in terms of access to information and communication, as well as new opportunities to exercise our rights and freedoms. But at the same time, we have seen that it is also digitisation that has increased the risks of human rights and personal data protection violations, including through abusive surveillance and unlawful data collection. Today, the digital process is guided by supranational, national and regional digital policies and is secured through national cybersecurity agendas focused on promoting overall economic growth and protecting critical information infrastructure and information security, but more attention needs to be paid to research the interests, needs and fears of people and communities who will now feel the application and effects of digitisation in their daily lives[16]. We have a mix of digital opportunities and threats. One of the vulnerabilities or one of the negative impacts of digitisation is that it can be used to violate human rights, in particular the right to privacy and freedom of expression, as proven by the number of cases involving this issue. E.g., governments and companies can collect and store personal data without the explicit consent of data subjects, which can lead to misuse or abuse of this information, and abusive surveillance can be used to restrict people's freedom of expression and association. We can see these developments through both a negative lens (of vulnerabilities) and a positive one (of benefits) digitisation can and has been used to protect human rights, to improve their lives and living conditions[17] and to improve access to information and justice, and here I can give as an example the use of blockchain technologies which can support the fight against corruption and the protection of property rights, while the use of artificial intelligence can better manage the identification and fight against discrimination. The main problems lie on the second side of the same coin, which I discussed when referring to vulnerabilities.

Personal data protection continues to be an important concern in the context of digitisation. States, public authorities and companies must now focus on respecting the right to privacy and protecting individuals' personal data. Personal data protection regulations, such as the European Union's General Data Protection Regulation, have been introduced precisely to ensure that this data is collected and used lawfully and responsibly.

---

[15] On 16 April 2014, the Committee of Ministers adopted Recommendation CM/Rec (2014)6 on Human Rights Guidelines for Internet Users. The material is available here: https://rm.coe.int/guide-to-human-rights-for-internet-users-romanian-/1680768064, and was accessed on 6.02.2023.

[16] Salminen, Mirva & Hossain, Kamrul, *Digitalisation and human security dimensions in cybersecurity: An Appraisal for the European High North. Polar Record, 54*(2), Ed. Cambridge University Press, 2018, pp. 108–118. doi:10.1017/S0032247418000268.

[17] One example is the coputerisation of farmland in many countries, which seems to have helped farmers and those interested. See details in Sabrin Beg, *Digitization and Development: Property Rights Security, and Land and Labor Markets*, in Journal of the European Economic Association, Volume 20, Issue 1 February 2022, pp. 395–429, https://doi.org/10.1093/jeea/jvab034.

3. Cyber security and current threats to digital security

Cyber security is a growing concern in the digital age, where almost every aspect of our lives is connected to the Internet. Threats to digital security are diverse and can have significant consequences for all subjects of international investment law and communications and new technologies law, be they individuals, legal entities or even states.

In this context we are mainly considering: 1) cyber attacks in their various forms: Malware (malicious software), phishing (email fraud), ransomware (blocking access to personal data and demanding ransom), and many others; 2) cyber espionage as a major threat to national security, in which foreign agents or hostile entities try to steal business secrets or military information; 3) industrial espionage in which competing companies try to steal business secrets or other sensitive information to increase their competitive advantage; 4) hacking as a personal or corporate threat, in which hackers attempt to break into computer systems or users' personal accounts to access personal or financial information; 5) disinformation and media manipulation through significant consequences on political and social processes, especially in the context of elections or other important events (which may manifest itself through the creation of false flags or fake news); and 6) 'cyber attention' and national sovereignty manifested by threats to national security by influencing government, organizations, or citizens in favor of hostile entities.

In the effort to combat these serious threats, common steps that can be taken include installing security software, using strong passwords, training employees on cyber threats, and implementing corporate or government security policies. Last but not least, international cooperation can be essential in combating digital security threats.

The role and responsibility of states, organisations and citizens in protecting human rights and digital security is a shared one, based on a series of actions such as implementing appropriate policies and regulations, promoting and protecting freedom of expression and free information in the digital space, preventing and combating threats to digital security, or drafting and implementing laws and regulations on the protection of personal data.

All participants in the legal relations of communications law and new technologies are involved in these actions. Legal entities, in particular manufacturers and service providers, have a responsibility to ensure that information provided to customers is accurate and not manipulative or misleading, or to respect human rights and promote business ethics.

Individuals need to protect their own personal information and be aware of cyber risks, not to spread false or manipulative information online, and to actively engage and demand that states and other entities protect their rights and take appropriate measures to prevent digital security threats. This is where the international responsibility and accountability of states come in. Individuals are encouraged to become more deeply involved in these actions, but viewed from a governance perspective it seems more effective for some urgent solutions to forego real citizen participation. An example was given by theory when it was observed that for smart city governance there is a perception that the inclusion of 'non-experts' is 'messy', time consuming and costly and therefore

does not align with the smart city's core principles of efficiency and cost reduction[18].

From a security, freedom and ethics perspective, ensuring a balance between human rights, digitisation and security can only be achieved by promoting a rights-based approach, by developing and implementing appropriate and flexible policies and regulations that are as responsive as possible to technological developments and new cyber threats, and by public education and awareness. Far from complete, these are based on the fact that mobile technologies, social media and increased connectivity are having a significant impact on the whole business and practice of human rights, as some of the literature has noted[19]. I refer including to the role of public information campaigns and the development of appropriate educational programmes, often with the support and initiative of international investors. One thing is certain: cyber threats know no borders and it is therefore important to have strong international collaboration to combat them in a targeted way. As I said at the beginning of this study, technological innovations can bring significant benefits to society, but they can also raise issues of human rights protection and security. 'Digital deterrence' or 'digital deterrence' (cyber deterrence is now also being discussed[20]) is a legal theory that argues that severe punishment and public deterrence of copyright infringement on the Internet are necessary to prevent such infringements in the future. This theory is based on the idea that illegally downloading and sharing music files and other content on the Internet can cause significant damage to copyright owners and can be considered a form of theft or piracy. In the United States, deterrence has been invoked several times in court in cases of copyright infringement on the Internet to motivate the award of significant damages and sometimes even criminal penalties. Many critics of digital deterrence have argued that it can lead to excessive penalties and that it can be misused with the effect of actually discouraging lawful and innovative activities in the field of technology and communications. It has been argued that harsh penalties are not always effective in preventing copyright infringement on the Internet, and that alternatives, such as more flexible content licensing, could be more effective and beneficial for all concerned.

'Until recently "cyberspace" was just a term in science fiction, and now our entire modern way of life, from communication to commerce to conflict, is fundamentally dependent on the Internet. (…) Most of all, cybersecurity issues affect us as individuals. We face new questions in everything from our rights and responsibilities as citizens in both the online and real world, to how to protect ourselves and our families from a new kind of danger.'[21]

---

[18] Tina Kempin Reuter, *Smart City Visions and Human Rights: Do They Go Together? Understanding the impact of technology on urban life*, Ed. Harvard Kennedy School Carr Center for Human Rights and Technology, issue 006, 2020, p. 4.

[19] Sam Dubberley, Alexa Koenig, Daragh Murray, *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, OUP-Oxford Public International Law, 2019, Part I, DOI: 10.1093/law/9780198836063.001.0001.

[20] We argue that the forthcoming debate on deterrence (sometimes used as a synonym for discouragement) can go in four directions: A greater incorporation of cyber deterrence as an element in the broader framework of international security and competition in a multi-domain world; a deeper focus on the technical aspects of the cyber domain to achieve deterrence effects at the operational and tactical level; a closer examination of compellence as an alternative form of coercion; and an exploration of new strategic concepts aimed at limiting and mitigating adversary aggression in cyberspace that depart from traditional deterrence thinking.

[21] For more debate on this topic, see Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar. What Everyone Needs to Know*, Oxford University Press, 2014, pp. 9–23.

4. General examples of good practices in the field of human rights protection and digital security in different countries and regions of the world

Estonia is known for developing a strong digital infrastructure and protecting human rights online, with a range of legal regulations and policies that protect human rights, including the right to privacy and the right to freedom of expression, along with a strong digital education programme that supports citizens to better understand how to protect their personal data, for example. Elsewhere, Canada has data protection regulations that protect human rights and digital security, define minimum standards of protection and provide penalties for breaches. The European Union has developed a set of rules and policies that protect human rights and digital security across the region, and I refer here to the General Data Protection Regulation (GDPR), which protects the personal data of European citizens, and the Cyber Security Directive, which imposes strict requirements to ensure the security of networks and information systems. They are joined by Japan, Brazil, China and South Africa. The European Union is active to promote cyber resilience, fight cyber crime and boost cyber diplomacy and cyber defence. Joint attempts to protect against cyber threats from third countries have resulted in a common diplomatic response called the 'cyber diplomacy toolkit' which includes diplomatic cooperation and dialogue, preventive measures against cyber attacks and some sanctions. The EU Cyber Security Strategy adopted by the European Commission and the EEAS in December 2020 strengthens the EU's diplomatic response to cyber attacks[22]. Also at EU level, the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union acts (Com/2021/206 final) was adopted.

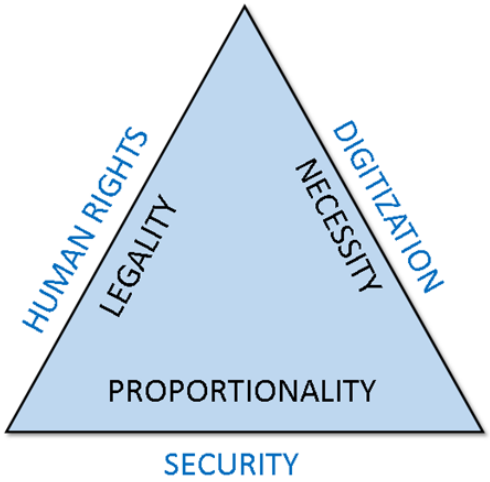
5. Implications of the New International Triangle for the economy, international investment, trade, education and other sectors of society

In terms of the economy, digitisation has led to increased efficiency and productivity in many sectors, such as e-commerce, financial services and manufacturing, but at the same time, digitisation has led to significant changes in the way companies operate as they are now more reliant on technology and data. Protecting personal data and cybersecurity are key to maintaining consumer confidence in using these digital services, which can have a direct impact on the economic success of companies. In commerce, digitisation has facilitated access to international markets and created business opportunities for companies of all sizes, although data protection and cybersecurity remain critical in protecting intellectual property and trade secrets. For education too, digitisation has opened up new opportunities for online learning and enabled global access to information and resources. The new International Triangle also has echoes for public policy and international relations. States need to find sustainable solutions and a balance between protecting human rights, ensuring cyber security and promoting economic growth, which is not easy.

The definitions and explanations of each component of the New International

[22] For more details see specific documents available on the Council of the European Union website, *Cybersecurity: how the EU tackles cyber threats*, available via this link: https://www.consilium.europa.eu/en/policies/cybersecurity/#diplomacy, accessed on 25.04.2023.

Triangle (human rights, digitization and security) and how they interact with each other are based on the observation that the triangle is in fact a modern paradigm of international relations that focuses on the interconnectedness of its three equal sides. In other words, following the same correspondence we can observe: legality, necessity and proportionality. Since I personally discovered this geometry, I named it 'DoDS Triangle' or, in English: 'HrDS triangle,' presenting it in the figure below:



Human rights are principles that protect human freedoms and dignity and are protected by international laws and treaties such as the UN Universal Declaration of Human Rights and the European Convention on Human Rights. We list in general terms the right to life, liberty and security of the person, the right to a fair trial, freedom of expression and opinion, the right to education, to work and to privacy. Digitisation is the transformation and adaptation of society to new technologies, including the use of the Internet, mobile devices, artificial intelligence, blockchain and other technological innovations. The way people communicate, work and interact with each other has already been changed and this process continues to develop rapidly. Alongside these, security is a complex concept, which refers to the protection of individuals, groups or nations against internal and external threats, based on a combination of laws, policies and specialised institutions, as well as physical or cyber security measures.

The interaction between the three components of the New International Triangle is strong and present in many forms. Digitisation can be used to promote and protect human rights, but it can also be a threat to them through illegal collection and storage of personal data or abusive surveillance. At the same time, security can be provided through data and information protection measures, but it can also be a threat to human rights, through the implementation of restrictive policies or the violation of the rights to privacy and free expression. Concerns have been raised about the impact on the privacy of facial recognition software, the risks of discrimination through replication or exacerbation of bias in AI systems, and the effects of some 'predictive policing' methods[23].

[23] Daniel Cullen, *Why Artificial Intelligence is Already a Human Rights Issue*, in Oxford Human Rights Hub (OxHRH Blog, 31 January 2018), material available here: https://ohrh.law.ox.ac.uk/why-artificial-intelligence-is-already-a-human-rights-issue, accessed 25.04.2023.

6. Possible trends and developments of the New International Triangle in the near future

All these interactions between personal data protection, algorithmic discrimination, electronic surveillance, online freedom of expression, access to information, information manipulation, legal liability, etc., can be better explored at a multidisciplinary and even transdisciplinary level, if we refer to law, information technology, ethics, psychology, public policy, diplomacy, military, economics and others. Algorithmic discrimination and the use of surveillance technologies such as facial recognition or online activity monitoring requires assessing the impact on human rights, analysing the risks and benefits, developing appropriate public policies to ensure a balance between security and respect for individual rights, collaborating between cybersecurity specialists, legal specialists, IT experts and ethicists to develop policies and technological solutions that protect human rights and ensure data security while identifying and addressing potential bias and discrimination in algorithms and artificial intelligence systems,

Given that these dynamics are in a constant state of flux, in the landscape of continuous advancement of technological development, the concern for personal data protection and privacy is expected to increase, leading to stricter data protection policies and greater responsibility of key actors (states and different legal entities) in their collection and use. In recent times, we have seen an increase in the number and severity of cyber-attacks, which has led to a greater awareness of the importance of cyber security and the channelling of attention and resources into developing cyber security technologies and strategies, as well as training and educating citizens about cyber risks. Undoubtedly, artificial intelligence (AI) will continue to develop and spread across sectors, which will have a significant impact on the New International Triangle through what we see as its advantages and disadvantages. Leading subjects of communications law and new technologies are likely to be increasingly called upon to take responsibility for protecting human rights and digital security, and for using digital technologies in a more responsible and sustainable way. New partnerships and global initiatives can be developed for the purpose of international cooperation to address common problems, such as the exchange of information and expertise and the development of international standards.

Human rights, digitisation and security are closely interlinked components, characterised by a complex interlinking dynamic, strongly influenced by political, economic and social changes around the world. If human rights, security and digitisation know no borders, then international law becomes the only regulatory space with the potential to be complete and sufficient. While international law was once considered a field separate from any influence of any other discipline, today it is increasingly inter- or transdisciplinary and intersects with other fields of knowledge such as political science, economics, sociology, philosophy and psychology. All fields of law are now confronted with this phenomenon.

We can therefore say that international law today enjoys universality. Traditionally, the universality of this field refers to international law as a global system of law, which has worldwide validity and is binding on all states. In this sense, the universality of international law refers primarily to the formal aspects of international

law and encompasses the form of the modern state and, with it, the principles of sovereign equality, non-intervention, peaceful coexistence and cooperation between independent states[24]. From this side, public international law presents itself as a recent *mathematics* of contemporary law. Historical developments have moved this field from its isolation to its universality today. Some authors consider that international law became universal when jurists from semi-peripheral polities, such as Japan, the Ottoman Empire and Latin American states, appropriated legal thinking from the European international[25]. We are witnessing the emergence of international law from anonymity to universality, amid the increasing interconnections between the subjects of this law[26]. This universality is in fact the direction towards the *transdisciplinary* destination, and represents a natural evolution given by society in transition. It can be said that transdisciplinarity and universality are mutually supportive in the fate of international law.

Transdisciplinarity is a solution finally proposed by this paper. It has the status of a research method[27] and is gaining increased attention in education, seeking to reduce the division that narrows disciplines and integrate the perspectives of different disciplines to better understand the complexities of the global system.

The intersection of communications law and the law of new technologies is of increasing interest to academics and practitioners. This is due to the rapid growth in the use of the Internet, mobile phones and social networks to facilitate communication and the emergence of new forms of legal regulation to govern these activities as comprehensively as possible. The *trans* approach seeks to examine the wider context in which these interact and their potential to reshape the way communication is regulated[28].

---

[24] André Nollkaemper, *Universality. Piracy – UNCLOS (UN Convention on the Law of the Sea) – Customary international law – Erga omnes obligations – Peremptory norms/ius cogens,* published under the auspices of the Max Planck Institute for Comparative Public Law and International Law under the direction of Professor Anne Peters (2021-) and Professor Rüdiger Wolfrum (2004–2020), product: Max Planck Encyclopedias of International Law [MPIL], Module: Max Planck Encyclopedia of Public International Law [MPEPIL] 2011, material available by subscription here: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1497, accessed 04.03.2023.

[25] See for details Arnulf Becker Lorca, *Universal International Law: Nineteenth-Century Histories of Imposition and Appropriation*, 51 Harvard International Law Journal 475, 2010; and Ward, Christopher, *The Universal Language of International Law: History and Prospects*, in Chinese (Taiwan) Yearbook of International Law and Affairs. Leiden, The Netherlands: Brill | Nijhoff. 2020, pp.6-13, DOI : https://doi.org/10.1163/978900 4443297_003.

[26] Charney, Jonathan I., *Universal International Law*, in The American Journal of International Law, vol. 87, no. 4, 1993, pp. 529-51. JSTOR, https://doi.org/10.2307/2203615.

[27] 'If in the case of multidisciplinarity we speak of a "correlation" of the efforts and potentialities of the different disciplines in order to provide as complete a view as possible of the objective under investigation, interdisciplinarity implies an intersection of different disciplinary areas (…) Transdisciplinarity represents the highest degree of curriculum integration, often going as far as fusion. Fusion is therefore the most complex and radical phase of integration.' Source is Cristina Stan, *Interdisciplinarity, transdisciplinarity and pluridisciplinarity in literature classes*, in Tribuna Învățământului of 5/10/2016, online, available here: https://tribunainvatamantului.ro/interdisciplinaritate-transdisciplinaritate-si-pluridisciplinaritate-in-cadrul-orelor-de-literatura/, accessed 05.03.2023.

[28] Antonia Rosetto Ajello, *Method of Knowledge and the Challenges of the Planetary Society: Edgar Morin's Pedagogical Proposal*, in World Futures, 61:7, 2005, pp. 511–533, DOI: 10.1080/02604020500283126.

7. Conclusions

We've seen the many human rights that have to do with digitisation. But how many ways is security in the same context? We can say that for each right there is a specific security measure. Paradoxically, security has its limits, which can be seen when situations arise in which there may be conflicts between security measures and human rights. Excessive monitoring of online communications or restricting access to certain online content can have a negative impact on freedom of expression or the right to privacy. Global digital inequalities, with certain groups or communities having limited access to technology or digital resources, can create inequalities in the protection of human rights in the digital environment, with some people being more vulnerable to security threats or violations of their rights online. Somehow, security seems to demand some sort of priority over digital human rights, and economic, political or security interests often influence policies and decisions, leading to trade-offs or prioritisation of certain interests over human rights protection.

And for international investment law, when a conflict arises between these two pieces that should harmoniously complement each other: security and human rights, the solution is to seek a balance so as to minimise the impact on the fundamental rights of individuals. The ideal starting point for any analysis is that security should be conducted in accordance with human rights principles and respect international human rights standards, such as the Universal Declaration of Human Rights and relevant international treaties. For these reasons, public international law can become overloaded with different regulatory proposals and this would not be a problem if there were sufficient institutions. As I have often said, this is where the importance of legal research and education comes in, because international law is not just foreign policy, but is perhaps the greatest laboratory known to mankind, in which the joint effort of specialists to analyse and re-establish boundaries through appropriate regulation comes first. From the confrontation between disciplines new results and new points between them emerge, and we can benefit from a new vision of Nature and Reality, which opens all disciplines to what they have in common and to what lies beyond their boundaries[29] considering the following guidelines: '1) considering that only an intelligence capable of understanding the planetary dimension of current conflicts could face the complexity of our world and the contemporary danger of the material and spiritual self-destruction of our species; 2) considering that life is seriously threatened by a triumphant technoscience which obeys only the unsustainable logic of efficiency in the service of efficiency; 3) considering that the contemporary rupture between an ever richer knowledge and an ever poorer inner being led to the emergence of a new obscurantism whose consequences on the individual and social level are incalculable; 4) considering that the accumulation of knowledge, unprecedented in history, accentuates the inequality between those who possess it and those who do not, thus causing inequality within nations and between nations on our planet; and 5) considering, at the same time, that all these dangers also have a positive counterpart, as the extraordinary growth of knowledge could eventually lead to a

[29] The Charter of Transdisciplinarity, adopted at the First World Congress on Transdisciplinarity, Convento da Arrábida, Portugal, 2–6 November 1994, paved the way for numerous studies that have made a huge contribution to the evolution of scientific research worldwide.

mutation comparable to that of the transformation of primates into Homo sapiens.[30] ’.

Bibliography

1. Beg, Sabrin, *Digitization and Development: Property Rights Security, and Land and Labor Markets*, in Journal of the European Economic Association, Volume 20, Issue 1 February 2022, pp. 395–429, https://doi.org/10.1093/jeea/jvab034.
2. Benöhr, Iris, *The Evolution of Consumer Protection and Human Rights*, EU Consumer Law and Human Rights, Oxford Studies in European Law (Oxford, 2013; online ed., Oxford Academic, 16 Apr. 2014), https://doi.org/10.1093/acprof:oso/9780199651979.003.0003, accessed 5 Feb. 2023.
3. Cait, Lamberton & Andrew, Stephen T., *A thematic exploration of digital, social media, and mobile marketing: Research evolution from 2000 to 2015 and an agenda for future inquiry* in Journal of Marketing, 80(6), 2016.
4. Charney, Jonathan I., *Universal International Law*, in The American Journal of International Law, vol. 87, no. 4, 1993, pp. 529-51. JSTOR, https://doi.org/10.2307/2203615.
5. Charter of Transdisciplinarity, adopted at the First World Congress on Transdisciplinarity, Convento da Arrábida, Portugal, 2–6 November 1994.
6. Council of the European Union, *Cybersecurity: how the EU tackles cyber threats*, available via this link: https://www.consilium.europa.eu/en/policies/cybersecurity/#diplomacy, accessed 25.04.2023.
7. Cullen, Daniel, *Why Artificial Intelligence is Already a Human Rights Issue*, in Oxford Human Rights Hub, (OxHRH Blog, 31 January 2018), material available here: https://ohrh.law.ox.ac.uk/why-artificial-intelligence-is-already-a-human-rights-issue, accessed 25.04.2023.
8. Dubberley, Sam; Koenig, Alexa & Murray, Daragh, *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, OUP-Oxford Public International Law, 2019, Part I, DOI: 10.1093/law/9780198836063.001.0001.
9. European Economic and Social Committee, *Digital transition must be fair: human rights and human control over the machine must remain fundamental values*, available online here: https://www.eesc.europa.eu/ro/news-media/news/tranzitia-digitala-trebuie-sa-fie-echitabila-drepturile-omului-si-controlul-uman-asupra-masinii-trebuie-sa-ramana-valori, accessed on 06.02.2023.
10. Gregorio, Giovanni de & Radu, Roxana, *Digital constitutionalism in the new era of Internet governance*, International Journal of Law and Information Technology, Volume 30, Issue 1, Spring 2022, Pages 68–87, https://doi.org/10.1093/ijlit/eaac004.
11. Kelley, Judith, *Assessing the Complex Evolution of Norms: The Rise of International Election Monitoring*, 62(2) International Organization, 2008, pp. 221–255, DOI: 10.1017/S0020818308080089.
12. Lorca, Arnulf Becker, *Universal International Law: Nineteenth-Century Histories of Imposition and Appropriation*, 51 Harvard International Law Journal, 475, 2010.
13. Nollkaemper, André, *Universality – Piracy – UNCLOS (UN Convention on the Law of the Sea) – Customary international law – Erga omnes obligations – Peremptory norms/ius cogens*, published under the auspices of the Max Planck Institute for Comparative Public Law and International Law under the direction of Professor Anne Peters and Professor Rüdiger Wolfrum (2004–2020).

[30] Ibid. See the preamble to the Charter.

14. OECD, *Rights in the digital age: Challenges and ways forward*, OECD Digital Economy Papers, No. 347, OECD Publishing, Paris, 2022, https://doi.org/10.1787/deb707a8-en.
15. Recommendation CM/Rec (2014)6 of the Committee of Ministers to member states on the Human Rights Guidelines for Internet Users and Explanatory Memorandum adopted by the Committee of Ministers on 16 April 2014.
16. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).
17. Reuter, Tina Kempin, *Smart City Visions and Human Rights: Do They Go Together? Understanding the impact of technology on urban life*, Ed. Harvard Kennedy School Carr Center for Human Rights and Technology, issue 006 2020.
18. Rosetto Ajello, Antonia, *Method of Knowledge and the Challenges of the Planetary Society: Edgar Morin's Pedagogical Proposal,* in World Futures, 61:7, 2005, pp. 511–533, DOI: 10.1080/02604020500283126.
19. Salminen, Mirva, & Hossain, Kamrul, *Digitalisation and human security dimensions in cybersecurity: An Appraisal for the European High North. Polar Record, 54*(2), Ed. Cambridge University Press, 2018, pp. 108–118. doi:10.1017/S0032247418000268.
20. Schmidt, Dennis R. & Trenta, Luca, *Changes in the law of self-defence? Drones, imminence, and international norm dynamics*, Journal on the Use of Force and International Law, 5:2, 2018, pp. 201–245, DOI: 10.1080/20531702.2018.1496706.
21. Singer, Peter W. and Friedman, Allan, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2014.
22. Stan, Cristina, *Interdisciplinarity, transdisciplinarity and pluridisciplinarity in literature classes*, in Tribuna Învățământului of 5/10/2016, online, available here: https://tribuna invatamantului.ro/interdisciplinaritate-transdisciplinaritate-si-pluridisciplinaritate-in-cadrul-orelor-de-literatura/, accessed on 05.03.2023.
23. Suseno, Yuliani & Nguyen, Doan T., *Culture is in the eye of the beholder: using metaphoric representations of cultural values to enhance consumer digital engagement*, Journal of Strategic Marketing (online), 2021, DOI: 10.1080/0965254 × .2021.1902373.
24. Viswanathan, Kumar; Vikram, Bhaskaran; Rohan, Mirchandani & Milap, Shah, *Creating a measurable social media marketing strategy: Increasing the value and ROI of intangibles and tangibles for hokey pokey* in Marketing Science, 32(2), 2013.
25. Ward, Christopher, *The Universal Language of International Law: History and Prospects*, in Chinese (Taiwan) Yearbook of International Law and Affairs. Leiden, The Netherlands: Brill | Nijhoff. 2020, pp. 6-13, DOI: https://doi.org/10.1163/9789004443297_003.