

RETHINKING RESPONSIBILITY IN THE DIGITAL AGE

Ilinca Bunescu
Alexandru Ioan Cuza University Iași
Year of study: 2nd

Abstract

This article examines how international law addresses responsibility in the context of artificial intelligence and digital technologies. Building on the jurisprudence of the International Court of Justice, it argues that responsibility is determined not by the immediate actor, but by the institutional and functional context in which conduct occurs. The analysis shows that AI systems do not constitute autonomous legal subjects but operate as tools within existing frameworks of attribution, control, and due diligence. At the same time, the growing influence of digital actors raises important questions regarding the protection of fundamental rights, as reflected in cases such as Google Spain and Gonzalez v Google.

The article concludes that traditional principles of international responsibility remain applicable in the digital age, provided they are carefully adapted to account for technological complexity and the transnational nature of digital environments.

1. THE LEGAL FRAMEWORK OF INTERNATIONAL RESPONSIBILITY

The starting point for any discussion on responsibility in international law is the identification of the legal subject capable of holding rights and obligations under the international legal order. International responsibility does not arise in the abstract but is attached to entities recognized as capable of bearing international obligations¹.

One of the foundational decisions in this regard is the advisory opinion delivered in *Reparation for Injuries Suffered in the Service of the United Nations*. In that opinion, the Court addressed whether the United Nations possessed the legal capacity to bring an international claim following the assassination of a UN mediator. The Court affirmed that the Organization possessed international legal personality and was therefore capable of asserting claims in its own name against the responsible Government with a view to obtaining the reparation due in respect of the damage caused to the Organization.²

¹ Crawford, J. (2019-07-09). *Brownlie's Principles of Public International Law*, Oxford University Press p.156–157.

² ICJ, *Reparation for Injuries Suffered in the Service of the United Nations*, Advisory Opinion, ICJ Reports 1949, p.174, p.179.

This reasoning is particularly significant because it demonstrates that the attribution of legal responsibility does not depend solely on the immediate physical actor responsible for the harm. Rather, the Court focused on the institutional interests and functions of the Organization. The injury suffered by the agent simultaneously impaired the functioning and authority of the United Nations itself. Consequently, the Organization could claim reparation not merely on behalf of the individual but for the protection of its own legal interests. The Court made this distinction explicit when clarifying the nature of the claim brought by the Organization. In the words of the Court, the Organization does not represent the agent, but is asserting its own right.³

The judgment therefore established an important doctrinal principle: international law recognizes the capacity of institutions to assert claims whenever their legally protected interests or functions are affected. The analysis does not stop at identifying the individual actor who physically performed the conduct, instead, it examines the broader legal framework within which that conduct occurred⁴. This approach becomes particularly relevant in situations where the immediate causal chain between actor and outcome is mediated through complex structures, whether institutional, technical, or operational.⁵

This principle was further articulated in the case concerning United States Diplomatic and Consular Staff in Tehran. In that case, the seizure of the United States embassy was initially carried out by militants who were not formally acting as organs of the Iranian state. Nevertheless, the Court concluded that Iran had violated its international obligations once it failed to take appropriate steps to protect the diplomatic mission and subsequently maintained the situation created by the militants. As summarized in the judgment, the Court concluded that the seizure of the Embassy was not initially imputable to the Iranian State, but that the State nevertheless incurred responsibility through its failure to take appropriate steps to protect the diplomatic premises and through the subsequent decision to maintain the situation so created.⁶ The law therefore recognizes that responsibility can arise not only from direct action but also from a state's failure to exercise control, supervision, or protection where international obligations require it.⁷

³ Ibidem, p.181.

⁴ Crawford, J. (2019-07-09). *Brownlie's Principles of Public International Law*, Oxford University Press p. 168-170.

⁵ Ibidem, p. 551.

⁶ ICJ, *United States Diplomatic and Consular Staff in Tehran (US v Iran)*, Judgment, ICJ Reports 1980, p.3, para 61–63.

⁷ Crawford, J. (2019-07-09). *Brownlie's Principles of Public International Law*, Oxford University Press p. 550-551.

Finally, the jurisprudence of the Court also confirms that domestic legal arrangements cannot override obligations arising under international law. This principle was clearly reaffirmed in the advisory opinion concerning the Applicability of the Obligation to Arbitrate under Section 21 of the United Nations Headquarters Agreement. In that dispute, the Secretary General challenged legislative measures adopted by the United States which were alleged to interfere with the functioning of the Permanent Observer Mission of the Palestine Liberation Organization to the United Nations. The Court emphasized that the existence of domestic legislative measures could not justify non-compliance with international obligations. As the proceedings revealed, the Secretary General maintained that international law prevails over domestic law and that obligations arising under the Headquarters Agreement must therefore be respected irrespective of domestic legislative measures.⁸

Taken together, these decisions establish several core principles that structure the law of international responsibility. First, responsibility attaches to entities possessing international legal personality and capable of bearing international obligations. Second, responsibility may arise not only from direct action but also from omissions⁹, failures of protection, or subsequent endorsement of harmful conduct. Finally, domestic legal arrangements cannot extinguish obligations arising under international law. These principles provide the doctrinal foundation upon which contemporary debates concerning technologically mediated conduct must be built.

2. AI AS TOOL, AI AS AGENT AND THE PROBLEM OF ATTRIBUTION

The emergence of artificial intelligence systems raises complex questions regarding the attribution of conduct in international law. The central question is not whether artificial intelligence can be considered an autonomous subject of international responsibility, but rather how responsibility should be attributed when technologically mediated conduct produces internationally relevant consequences.

⁸ Applicability of the Obligation to Arbitrate under Section 21 of the United Nations Headquarters Agreement of 26 June 1947, Advisory Opinion, I.C.J.Reports 1988, p.12.

⁹ Ibidem.

2.1. AI as an instrument of State or institutional action

The jurisprudence of the International Court of Justice suggests that the attribution of conduct in international law is primarily concerned with the institutional framework within which the conduct occurs.¹⁰ In other words, the legal analysis focuses less on the immediate factual actor and more on the entity exercising authority, control, or institutional function.¹¹

This functional approach is reflected in the Court's reasoning in the advisory opinion concerning the immunity of a Special Rapporteur of the Commission on Human Rights. In that case, the Court emphasized the central role of the Secretary-General in determining whether the conduct of an expert fell within the scope of his official mission. The Court noted that the Secretary-General, as the chief administrative officer of the Organization, has a pivotal role in determining whether an expert on mission acted in the course of his mission.¹² The significance of this reasoning lies in the fact that the Court did not focus exclusively on the personal actions of the individual expert. Instead, it examined whether those actions were sufficiently connected to the institutional mission entrusted to him by the United Nations. The legal characterization of the conduct therefore depended on its relationship with the functions and authority of the Organization.¹³

This functional logic can be extended to situations involving artificial intelligence systems. When a state or an international organization deploys an AI system in the exercise of its functions, whether for administrative decision-making, regulatory enforcement, or operational analysis, the resulting conduct cannot be viewed in isolation from the institutional framework in which the system operates. The relevant legal question is not whether the algorithm itself possesses agency, but whether the conduct generated by the system forms part of the institutional activity of the entity that deployed it.

2.2. The Blackbox problem

A common argument in discussions surrounding artificial intelligence concerns the so-called blackbox problem. Complex machine-learning systems may produce outputs that are difficult to explain or trace to a specific human decision. While such opacity may create

¹⁰ Ibidem.

¹¹ Ibidem, p. 558-559.

¹² Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights, ICJ Reports 1999, p. 62, para 61.

¹³ Crawford, J. (2019-07-09). Brownlie's Principles of Public International Law, Oxford University Press, p. 169-170.

practical challenges for evidence and oversight, it does not fundamentally alter the legal structure of responsibility in international law.

International law has long required states and international actors to comply with their obligations in good faith and to ensure that their internal arrangements do not undermine those obligations.¹⁴ This principle was emphasized in the Rainbow Warrior arbitration, where the tribunal reaffirmed the binding nature of international commitments and the obligation to perform them in good faith. As the tribunal explained, the principle of good faith is one of the basic principles governing the creation and performance of legal obligations.¹⁵

The relevance of this principle in the context of artificial intelligence is clear. States cannot rely on the complexity of technological systems as a justification for evading their international obligations. The existence of sophisticated algorithms, automated decision making systems, or opaque computational processes does not dissolve the responsibility of the state or organization that designed, implemented, or relied upon those systems. In this sense, technological opacity may complicate the factual reconstruction of events, but it does not create a legal void in which responsibility disappears.¹⁶ The obligations of states remain anchored in their duty to exercise control over the mechanisms through which their policies and decisions are implemented.

2.3. Failure to control autonomous systems

Another important dimension of international responsibility concerns omissions and failures to act. Responsibility may arise not only from direct actions of state organs but also from a state's failure to exercise due diligence¹⁷ in preventing harm or protecting legally protected interests.

This principle was clearly articulated in the judgment concerning the seizure of the United States Embassy in Tehran. Although the initial takeover of the embassy was carried out by militant groups that were not acting as organs of the Iranian state, the Court nevertheless concluded that Iran had breached its international obligations. The Court explained that the Court concluded that the seizure of the Embassy was not initially imputable to the Iranian State, but that the State nevertheless incurred responsibility through its failure to take appropriate

¹⁴ Rainbow Warrior Arbitration, 30 April 1990 VOLUME XX pp. 215-284, p.251.

¹⁵ Rainbow Warrior Arbitration, 30 April 1990 VOLUME XX pp. 215-284, p.251-256.

¹⁶ Crawford, J. (2019-07-09). Brownlie's Principles of Public International Law, Oxford University Press, p. 551.

¹⁷ Ibidem.

steps to protect the diplomatic premises and through the subsequent decision to maintain the situation so created. The Tehran case illustrates that international responsibility may arise even when the original act cannot be directly attributed to a state organ.¹⁸ What becomes decisive is the state's subsequent conduct and its failure to fulfil obligations of protection, supervision, or prevention.

In the context of artificial intelligence, this reasoning has direct implications. If a state deploys autonomous systems that influence or determine decisions affecting individuals, infrastructure, or international relations, the state retains a duty to supervise and control¹⁹ the operation of those systems. A failure to establish adequate safeguards, monitoring mechanisms, or corrective procedures could therefore give rise to responsibility where harmful outcomes occur.²⁰

2.4. Subsequent adoption of algorithmic decisions

Closely related to the notion of failure to control is the concept of subsequent adoption of conduct.²¹ Even when the initial act originates from actors outside the formal structure of the state, responsibility may arise if the state later endorses or maintains the resulting situation.

This reasoning has particular relevance for systems involving automated or algorithmic decision making. Artificial intelligence systems often produce recommendations, classifications, or predictions that are subsequently adopted by human authorities. Once a state authority accepts, validates, or implements such outputs as part of its official decision-making process, those outputs effectively become part of the conduct of the state.²² Thus, the presence of algorithmic mediation does not interrupt the legal chain of attribution. The decisive factor remains whether the state has integrated the output of the system into its own institutional actions or policies.

2.5. Technological mediation and the continuity of attribution

Taken together, the jurisprudence of the International Court of Justice demonstrates that international law is well equipped to deal with technologically mediated conduct. The presence

¹⁸ ICJ, *United States Diplomatic and Consular Staff in Tehran (US v Iran)*, Judgment, ICJ Reports 1980, 3, para 61–63.

¹⁹ Crawford, J. (2019-07-09). *Brownlie's Principles of Public International Law*, Oxford University Press, p. 551.

²⁰ *Ibidem*.

²¹ *Ibidem*, p. 550-551.

²² *Ibidem*.

of complex intermediaries, whether human agents, institutional mechanisms, or technological systems, does not prevent the attribution of responsibility.

Instead, the law focuses on a series of structural questions: who authorized the system²³, who deployed it²⁴, who relied on its outputs, and whether adequate mechanisms existed to supervise or correct its operation. These questions reflect the broader functional approach that has long characterized the law of international responsibility. In this respect, artificial intelligence does not fundamentally transform the legal structure of responsibility. It merely introduces a new form of mediation between institutional decision-makers and the resulting conduct. The core principles established in the jurisprudence of the Court, functional analysis, institutional responsibility, and the continuing duty of control, remain fully applicable.

3. RESPONSIBILITY OF DIGITAL ACTORS AND PROTECTION OF INDIVIDUALS IN THE DIGITAL ENVIRONMENT

The rapid expansion of digital technologies has transformed the manner in which information is collected, processed, and disseminated worldwide. The role played by digital intermediaries has been recognized by courts as extending beyond that of a purely passive conduit of information. In particular, search engines actively collect, organize, and structure information available online, thereby influencing how it becomes accessible to the public. As the Court of Justice of the European Union explained when examining the functioning of search engines, the activity of a search engine consists in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference.²⁵

Because of this active role in structuring access to information, search engines may significantly amplify the dissemination of personal data. The Court emphasized that the aggregation and indexing of information by a search engine can have a greater impact on the rights of individuals than the original publication itself. As the Court noted, the processing of personal data carried out in the context of the activity of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data.²⁶

²³ Ibidem.

²⁴ Ibidem, p. 558-559.

²⁵ CJEU, Google Spain, Case C-131/12, para 28.

²⁶ CJEU, Google Spain, Case C-131/12, para 80-81.

This recognition reflects a broader understanding that digital actors are capable of exercising real influence over the enjoyment of fundamental rights in the online environment. Contemporary international instruments confirm that the protection of human rights must extend fully into the digital sphere. In this regard, States have reaffirmed that all human rights must be respected, protected and promoted online and offline.²⁷

However, the existence of such influence does not automatically establish legal liability for every harmful act committed through digital platforms. Courts have also emphasized that responsibility must be assessed carefully and on the basis of concrete legal standards. In particular, liability cannot be inferred solely from the fact that third parties use a digital platform to disseminate harmful content. In a case concerning allegations that an online platform facilitated terrorist activity, the Supreme Court of the United States observed that the plaintiff's allegations failed to state a viable claim for aiding and abetting liability, emphasizing that the mere operation of a platform through which third parties disseminate content does not automatically establish legal responsibility.²⁸ These developments illustrate the emergence of a balanced legal framework governing digital technologies. On the one hand, courts and international instruments recognize the considerable influence exercised by digital intermediaries in shaping access to information and the resulting implications for fundamental rights. On the other hand, legal responsibility must remain grounded in established principles of law, ensuring that liability is not imposed solely because a digital platform facilitates the circulation of information generated by third parties.

Accordingly, the regulation of digital actors must pursue a careful balance between the protection of individual rights, the preservation of freedom of expression, and the continued development of innovative digital technologies.

4. INTERNATIONAL RESPONSIBILITY AND THE DUTY TO PREVENT HARM IN THE DIGITAL ENVIRONMENT

International law establishes that States are not only responsible for their own conduct but may also incur responsibility where they fail to prevent harmful acts occurring within their jurisdiction or under their control. This principle reflects a broader obligation of due diligence

²⁷ UNGA, Global Digital Compact, UN Doc A/79/L.2 (2024).

²⁸ *Gonzalez v Google LLC*, 2023

requiring States to ensure that activities carried out within their territory do not cause harm to other States or undermine the international legal order.²⁹

The International Court of Justice has repeatedly confirmed that States must refrain from allowing their territory to be used for activities contrary to international law. In its landmark judgment in *Military and Paramilitary Activities in and against Nicaragua*, the Court reaffirmed the fundamental rule that no State may use or encourage the use of force by irregular forces or armed bands against another State.³⁰ Beyond prohibiting direct involvement, international law also imposes obligations of prevention. State responsibility may arise not only through direct participation in unlawful acts but also through a failure to take the necessary measures to prevent them. The International Court of Justice clarified the scope of this obligation in *Bosnia and Herzegovina v Serbia and Montenegro*, where it emphasized that the duty to prevent arises whenever a State possesses the capacity to influence the relevant actors. As the Court explained, a State's obligation to prevent is one of conduct and not one of result, therefore the State is required to employ all means reasonably available to them, so as to prevent genocide so far as possible.³¹

This reasoning reflects the broader doctrine of due diligence in international law.³² States must take reasonable steps to prevent harmful activities emanating from their territory or from actors subject to their jurisdiction. Such obligations are particularly significant in contexts where private actors may generate cross-border consequences. Even when harmful conduct is carried out by non-state actors, international law requires States to adopt appropriate regulatory and supervisory frameworks capable of mitigating such risks.

These considerations are increasingly relevant in the context of digital technologies and transnational digital platforms. The activities of digital actors may have immediate global effects³³, influencing the circulation of information, economic relations, and even public security across borders. Consequently, emerging international governance frameworks recognize the need for responsible oversight of digital technologies. As recently reaffirmed in global discussions on digital governance, States have committed to ensuring that technological development remains consistent with international law and human rights. In particular, it has

²⁹ Crawford, J. (2019-07-09). *Brownlie's Principles of Public International Law*, Oxford University Press, p. 456-458

³⁰ *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States)*, ICJ Reports 1986, para 202.

³¹ ICJ, *Bosnia Genocide Case, Bosnia and Herzegovina v Serbia and Montenegro*, ICJ Reports 2007, para 430.

³² Crawford, J. (2019-07-09). *Brownlie's Principles of Public International Law*, Oxford University Press, p.551.

³³ Crawford, J. (2019-07-09). *Brownlie's Principles of Public International Law*, Oxford University Press, p.460.

been emphasized that all human rights must be respected, protected and promoted online and offline.³⁴

At the same time, international cooperation remains an essential component of addressing challenges arising from the digital environment. The transnational nature of digital technologies requires coordinated legal and regulatory responses, as isolated national measures may prove insufficient to address harms that transcend jurisdictional boundaries. International legal instruments therefore stress the importance of collaborative governance involving States, international organizations, and private stakeholders in order to ensure a secure and rights-respecting digital environment.

Accordingly, the evolving digital landscape does not diminish the relevance of traditional principles of international responsibility. On the contrary, the emergence of powerful digital actors reinforces the importance of the duty of due diligence. States remain responsible³⁵ for adopting reasonable measures to prevent harmful activities³⁶ originating within their jurisdiction, particularly where such activities may produce transnational effects and threaten the protection of fundamental rights or the stability of the international legal order.

5. MODERN TECHNOLOGY JURISPRUDENCE AND THE EVOLUTION OF LEGAL RESPONSIBILITY

The rapid development of digital technologies has generated profound transformations in the legal landscape, prompting scholars and courts alike to reconsider how traditional legal principles apply in technologically mediated environments. These developments raise complex questions regarding accountability, transparency, and legal responsibility. As scholars have noted, the increasing use of algorithmic decision-making systems raises fundamental questions regarding transparency, accountability and the allocation of legal responsibility.³⁷

The growing influence of digital technologies has also contributed to the emergence of the concept known as digital constitutionalism. This approach seeks to apply core constitutional principles, such as the protection of fundamental rights, the rule of law, and democratic accountability to the governance of digital platforms and online environments. Within this framework, digital platforms are increasingly understood not merely as private intermediaries

³⁴ UNGA, Global Digital Compact, UN Doc A/79/L.2 (2024).

³⁵ Crawford, J. (2019-07-09). Brownlie's Principles of Public International Law, Oxford University Press, p.551.

³⁶ Ibidem

³⁷ Yeung K, Algorithmic Regulation (2017), p.14, available at: https://www.researchgate.net/publication/318820255_Algorithmic_regulation_A_critical_interrogation, accessed on: 14.01.2026, at 18:22.

but as actors exercising significant power over the digital public sphere. As scholars have observed, digital constitutionalism refers to the effort to articulate a set of political rights, governance norms and limitations on the exercise of power in the digital environment.³⁸

Courts have played a particularly significant role in shaping this emerging legal framework. For example, in addressing the role of search engines in the dissemination of personal information, the Court of Justice of the European Union emphasized the active role played by such platforms in organizing and structuring online content. The Court explained that the activity of a search engine consists in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference.³⁹

The Court further recognized that the processing of information by digital intermediaries may significantly affect the enjoyment of fundamental rights. In particular, it observed that the processing of personal data carried out in the context of the activity of a search engine is liable to significantly affect the fundamental rights to privacy and to the protection of personal data.⁴⁰

These developments illustrate the gradual emergence of a broader paradigm of technological responsibility within contemporary legal systems. Rather than treating technological systems as legally neutral tools, modern legal analysis increasingly recognizes that digital infrastructures shape the distribution of power, access to information, and the protection of individual rights.⁴¹ Consequently, the allocation of responsibility must take into account the complex interactions between states, private actors, technological systems, and international legal frameworks.⁴²

In this evolving landscape, modern technology jurisprudence does not seek to replace traditional legal principles but rather to reinterpret them in light of technological transformation. Established doctrines such as responsibility, accountability, and due diligence remain central to legal analysis⁴³, yet their application must reflect the realities of algorithmic governance and the increasing influence of digital platforms on social, economic, and political life. As a result,

³⁸ Celeste E, Digital Constitutionalism (2022), available at: <https://www.taylorfrancis.com/reader/read-online/0ab0f99a-fa7c-47f2-9cdf-a12b14e52d98/book/epub?context=ubx>, accessed at: 12.02.2026, at 19:23.

³⁹ Google Spain v AEPD and Mario Costeja González, p. 12.

⁴⁰ Ibidem, p.13.

⁴¹ Crawford, J. (2019-07-09). Brownlie's Principles of Public International Law, Oxford University Press, p.447-448.

⁴² Ibidem, p.551.

⁴³ Ibidem.

contemporary legal scholarship increasingly emphasizes the need for legal frameworks capable of ensuring that technological innovation remains compatible with the protection of fundamental rights and the broader principles of the international legal order.⁴⁴

CONCLUSIONS

The rapid expansion of digital technologies and artificial intelligence systems represents one of the most profound transformations affecting contemporary legal systems. Digital infrastructures increasingly shape the circulation of information, the functioning of economic markets, and the exercise of fundamental rights across national borders.⁴⁵ This article has demonstrated that existing principles of international law remain capable of addressing many of the challenges posed by digital technologies. Doctrines such as state responsibility, due diligence⁴⁶, and the protection of fundamental rights continue to provide a solid normative foundation for regulating the digital sphere.

At the same time, the emergence of powerful digital actors and algorithmic systems introduces new layers of complexity into the allocation of legal responsibility. The growing body of scholarship on technology jurisprudence⁴⁷ and digital constitutionalism⁴⁸ reflects this shift in legal thinking. These emerging approaches seek to adapt traditional legal frameworks to the realities of algorithmic governance, emphasizing the need to ensure that technological development remains consistent with fundamental rights, democratic values, and the rule of law. In this context, courts have played an increasingly important role in shaping legal standards capable of addressing the challenges posed by digital technologies.

Ultimately, the central task facing contemporary legal systems is therefore not the creation of entirely new legal orders but the careful adaptation of established principles⁴⁹ to an increasingly interconnected and technologically mediated world. Ensuring that digital innovation remains compatible with human dignity, legal certainty, and the protection of fundamental rights⁵⁰ will require sustained cooperation between states, international institutions, courts, and private actors. In this sense, the law is not merely reacting to

⁴⁴ Ibidem, p.459-460.

⁴⁵ Ibidem.

⁴⁶ Ibidem, p.551.

⁴⁷ Yeung K, Algorithmic Regulation (2017), available at: https://www.researchgate.net/publication/318820255_Algorithmic_regulation_A_critical_interrogation, accessed on: 19.02.2026, at 20:50.

⁴⁸ Celeste E, Digital Constitutionalism (2022), <https://www.taylorfrancis.com/reader/read-online/0ab0f99a-fa7c-47f2-9cdf-a12b14e52d98/book/epub?context=ubx> .

⁴⁹ Crawford, J. (2019-07-09). Brownlie's Principles of Public International Law, Oxford University Press, p.551.

⁵⁰ ibidem, p.460.

technological change, it is actively shaping the normative boundaries within which technological progress unfolds. The challenge of the digital age therefore lies not in choosing between innovation and regulation, but in ensuring that technological advancement continues to serve the broader objectives of justice, accountability, and the rule of law in an increasingly digital world. Even in an era defined by artificial intelligence and digital networks, the central mission of legal systems remains the protection of human dignity, the preservation of accountability, and the safeguarding

BIBLIOGRAPHY

I. Doctrine

1. Cassese, Antonio, *International Law* (2nd edn, Oxford University Press 2005).
2. Crawford, James, *Brownlie's Principles of Public International Law* (9th edn, Oxford University Press 2019).
3. Shaw, Malcolm Nathan, *International Law* (8th edn, Cambridge University Press 2017).

II. Specialized articles and studies

1. Balkin, Jack M, 'Free Speech in the Algorithmic Society' (2018) 51 UC Davis Law Review 1149, https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-3_Balkin.pdf.
2. Yeung, Karen, *Algorithmic Regulation: A Critical Interrogation* (2018), https://www.researchgate.net/publication/318820255_Algorithmic_regulation_A_critical_interrogation.

III. Sources in electronic format

1. Celeste, Edoardo, *Digital Constitutionalism: The Role of Internet Bills of Rights* (Routledge 2022), <https://www.taylorfrancis.com/reader/read-online/0ab0f99a-fa7c-47f2-9cdf-a12b14e52d98/book/epub?context=ubx>.
2. United Nations General Assembly, *Global Digital Compact UN Doc A/79/L.2* (2024), https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf.

IV. Case law

1. *Applicability of the Obligation to Arbitrate under Section 21 of the United Nations Headquarters Agreement of 26 June 1947* (Advisory Opinion) ICJ Reports 1988.
2. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* (Judgment) ICJ Reports 2007.
3. *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights* (Advisory Opinion) ICJ Reports 1999, 62.
4. *Gonzalez v Google LLC* 598 US (2023).
5. *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Case C-131/12).
6. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) ICJ Reports 1986, 14.
7. *Rainbow Warrior Arbitration (New Zealand v France)* (1990) 20 RIAA 215.
8. *Reparation for Injuries Suffered in the Service of the United Nations* (Advisory Opinion) ICJ Reports 1949, 174.
9. *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)* (Judgment) ICJ Reports 1980, 3.

V. Legislation

1. Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945).