Dilemmas and Dispute Resolution of Human Rights Guarantees in the United Nations Convention Against Cybercrime: From the Perspective of the Scope of Criminalisation

Siyuan Qu
Administrative Law School, Southwest University of Political Science and Law, Chongqing, China

Keywords: Criminalisation, UN, Cybercrime, Human Rights.

Abstract: The development of cybertechnology and the increasing frequency of cross-border interactions have made cybercrime a major challenge in both public and private law. The United Nations Convention against Cybercrime, which was concluded after many rounds of negotiations to fully coordinate different concerns of countries, is not only a great achievement in the global governance of cybercrime, but also a brilliant breakthrough in the difficult period of multilateralism. The human rights controversy over the convention has long existed but has been less studied, and the failure to clarify the ambiguity will most likely affect the subsequent entry into force and implementation. Through comparative and interpretative research methods, comparing the claims of both broad and narrow criminalisation patterns, and focusing on the existing provisions of the convention to analyse the reality of its criminalisation scope, the study finds that the convention is not in fact a product dominated by a broad criminalisation pattern. In adher-ing to the stance of combating cybercrime while taking into account human rights safeguards to the greatest extent possible, a good job in coordinating with domestic laws for the convergence and harmoni-sation of the convention and setting up a bona fide research exception term can provide reference for the subsequent improvement of it and the formulation of its draft supplementary protocol, contributing to the better coordination of the interests of parties and responding to the purpose of combating cybercrime eventually.

1 INTRODUCTION

1.1 Conclusion of the Convention

The background of the times, in which criminal offences have become more and more rampant in virtual space and in which multilateralism and unilateralism are at war, provided the basis for the birth of *the United Nations Convention against Cybercrime* (hereinafter referred to as "*the Convention*") and the necessity for its subsequent implementation. In recent years, technological innovations and cross-border interactions have fuelled the free flow of information and sharing of resources, while at the same time providing a breeding ground for cybercrime by taking advantage of public health emergencies and other crises (Albader, 2022), posing serious challenges to the international interests and domestic governance of countries. Therefore, seeking an authoritative and stable cooperation system at the international level to coordinate the interests of multiple parties has become a breakthrough recognised by most countries. The United Nations General Assembly adopted *the Convention* on 24 December 2024, as the first universal international convention formulated under the auspices of the United Nations in terms of global governance of crimes in cyber-virtual space, which is highly cohesive of the consensus of multinational cooperation and bridges the differences in the legislation among countries (Jiang, 2023), providing a systematic legal framework for combating cybercrime in today's world where criminal offences are increasingly rampant on the basis of digital networks. And that, it once again proves the superiority of multilateralism in dealing with global challenges and provides a reference for other international issues that need to be addressed urgently, particularly when pseudo-multilateralism is posting a threat to world peace.

Qu, S.
Dilemmas and Dispute Resolution of Human Rights Guarantees in the United Nations Convention Against Cybercrime: From the Perspective of the Scope of Criminalisation.
DOI: 10.5220/0014293100004859

In *Proceedings of the 1st International Conference on Politics, Law, and Social Science (ICPLSS 2025)*, pages 13-19
ISBN: 978-989-758-785-6

1.2 Dispute and Resolution

The various focuses on the value positions, institutional needs and ecological foundations of cybercrime governance among the participating parties have given rise to a variety of major games and focal issues in the formulation and implementation of *the Convention* (Wu, 2025). Opponents believe that *the Convention,* in which the concept of cybercrime and legislation are broad and universal (Chalana & Bhanu, 2024), is likely to be maliciously exploited by some countries and that it should not be ratified because of its shortcomings of violating human rights, endangering security, suppressing freedom and hindering development. Among them, compared with international cooperation and technology governance issues, which are the main research hotspots, the controversy over human rights is particularly prominent but less targeted research. The concern of human rights mainly focuses on the belief that the scope of criminalisation of *the Convention* is so broad, leading to the over-interference in human rights. Therefore, if we do not base our analysis on the specific text of *the Convention* to resolve the disagreements in criminalisation, find a point of balance between broad and narrow criminalisation patterns to safeguard human rights, respond to and resolve the suspicion that broad criminalisation is detrimental to human rights, and guide the return to the fundamental purpose of combating cybercrime, the flaws in the design of the human rights guarantee system will be the main ground for the opposing parties to level malicious accusations against *the Convention* (*Secrss*, 2024). This will strengthen the risk of "group polarisation", which in turn will affect the ultimate effectiveness of the first attempt to develop a universal convention in the cyber and digital domains (*Secrss*, 2024). At the same time, given that *the Convention* has not yet formally entered into force, timely amendment and improvement of the relevant provisions or relevant explanations will help more subjects to understand the purpose of *the Convention*, eliminate relevant concerns and actively participate in signing. Therefore, in order to facilitate the formal entry into force of *the Convention*, and provide a reference for its subsequent refinement and for the formulation of the draft supplementary protocol, this study uses comparative and interpretative research methods to explore the reality of the criminalisation scope of *the Convention* on the basis of its specific provisions, to sort out and respond to existing disputes, and to provide paths for its improvement.

2 THE DICHOTOMY BETWEEN THE CLAIMS OF BROAD AND NARROW CRIMINALISATION

Criminalisation is a complex social issue that requires a reasonable and effective balance between order maintenance and human rights guarantee. Overly broad criminalisation standards may lead to the conviction of innocent people and, conversely, may fail to respond to the law-making purpose of effectively combating crime.

2.1 Broad Versus Narrow Criminalisation

China, the Russian Federation and other countries advocate the broad criminalisation pattern, believing that the scope of criminalisation under *the Convention* should be as comprehensive as possible to cover offences committed through the use of the Internet, such as telecommunication network fraud. At the same time, given that *the Convention* itself has not responded to the new problems posed by the development of new technologies, such as artificial intelligence, it should be revised in a timely manner in accordance with the needs of practice and technological changes, expand the types of offences in due course, and improve the framework by means of supplementary protocols (Wu, 2025).

States parties to the Budapest Convention, represented by European and American countries, supported the narrow criminalisation pattern. They claim that an overly broad scope of cybercrime entailed the risk of unduly interfering with human rights and consider that the scope of criminalisation should be limited to offences committed against computer systems and the idea of expanding the scope of criminalisation must be adopted with caution (Wu, 2025). For example, Germany argued that the expansion of the scope of cybercrime to all crimes committed with computers should be considered with caution, as the use of computers to commit crimes was not necessarily cybercrime (Zhang & Gong, 2020). At the same time, they insisted on the principle of "technological neutrality", with a view to making the legal framework of the *Convention* inclusive of technological developments and avoiding frequent revisions that would undermine the relative stability of the rules (Wu, 2025).

2.2 Causes of Confrontation

2.2.1 Immediate Causes: The Broadness of the Concept of Cybercrime

Chapter II of *the Convention*, entitled "Interpretation of terms", does not define cybercrime, although it clarifies the meaning of many words and phrases in the context of cybercrime for the purpose of defining the nature of the acts in question. Taking into account the lagging nature of the law, the majority of countries have not clearly defined the concept of cybercrime at the legislative level, although some of them have interpreted it in their effective judicial practice in very broad terms for purposes of underpinning. At the same time, the forms and means of cybercrime are constantly evolving. As a result, the long-term absence of a uniform framework of rules, coupled with the complexity and diversity of cybertechnology, has made it difficult to resolve the problem of the broad concept of cybercrime. Moreover, there are differences in the perceptions of cybercrime in various sectors of society, and there are various preferences between severe punishment, education and rehabilitation. To a certain extent, these have led to differences in the value stance and factors to be considered by countries in the management of cybercrime, which in turn affects the development of the two propositions of scope of criminalisation.

2.2.2 Root Causes: The Choice between Security and Human Rights

The focus between security and human rights is key to distinguishing between broad and narrow patterns of criminalisation, representing the core values of each. The immediate reason represented by the broadness of the concept of cybercrime is simply to serve as a vehicle to provide a platform for adding one's own values to the two propositions.

The desire of countries to form joint efforts in the international community to combat crime is based on the consideration that, on the one hand, it is proactive in safeguarding the security of the country and its people, so that, in the event of a threat to security, the appropriate subjects can be punished in accordance with international rules. On the other hand, it is a passive way to improve the means of redress, that is, in the event that security is violated by any foreign infringement, redress is available in accordance with the rules and the state of security is restored. Sovereignty just establishes a reasonable balance between the hopes of States. Thus, both the fight against crime and the emphasis on and protection of sovereignty can be understood in most international contexts as an emphasis on national security.

The universality pursued by *the Convention* determines that the principles of human rights and sovereignty have become its two basic principles, and the game between the two was played throughout the negotiation process of *the Convention*. China, Some countries have consistently insisted that the principle of sovereignty should be applied to cyberspace as a prerequisite for the protection of the security of the country as well as the people's personal property in the virtual space. However, Western countries, represented by the United States and EU member states, based on ideological traditions, glorify freedom, highlight human rights protection, and even downplay the importance of national sovereignty (Wu, 2025). They argue that some criminal convictions and procedures and law enforcement measures infringe on privacy and freedom of expression (Tropina, 2024). Although the notion of respect for and preservation of human rights is recognized by the majority of countries, there is still a substantial variation in the understanding of the relationship between human rights, sovereignty and the battle against cybercrime among them (Wu, 2025).

3 RESPONSE AND SETTLEMENT OF DISPUTES

The essence of international communication is cooperation and conflict. Being in the stage of the situation, in the face of the suspicion of the deficiencies of the human rights protection of *the Convention* due to the overly broad conviction, we should conduct a detailed analysis based on the existing provisions of *the Convention*, seek a compromise to correctly deal with the contradiction between the increasingly serious situation of cybercrime and the highlighted need for human rights protection, and return to the original intention of gathering international strength to combat crime and protect the citizens of the world.

3.1 Observations: The Reality of the Scope of Criminalisation of

One of the main obstacles to establishing a common strategy for international harmonisation in the area of cybercrime has been the lack of a consensus over whether acts qualify as this kind of criminality (Tropina, 2024). The hasty aggregation of national

forms of criminalisation will inevitably lead to an expansion of the scope of domestic criminalisation in multiple countries, leading to a range of problems such as abuse of power, overpunishment and ineffective governance. Just operating simple intersection calculation will also foresee realities that are incompatible with the domestic context, such as fish escaping from the net, ineffective crackdowns and declining public trust, and may infringe on the human rights of a wider range of potential victims. While *the Convention*'s middle-of-the-road approach has temporarily calmed the interests of many, its subsequent implementation remains a great challenge. The controversy over human rights guarantees is now highlighted in the game between the broad and narrow criminalisation patterns. The overly broad criminalisation which leads to excessive interference of human rights has been the focus of criticism of *the Convention* by advocates of the narrow criminalisation pattern. In this context, it is necessary to return to the specific provisions of *the Convention* for practical analysis.

3.1.1 List of Offences

Chapter II of *the Convention*, entitled "Criminalisation", covers a total of 11 criminal entities, including Illegal access, Interference with electronic data, Offences related to online child sexual abuse or child sexual exploitation material, Non-consensual dissemination of intimate images and laundering of proceeds of crime and so on. In addition, it also includes content about specific identification of liability of legal persons, participation and attempt.

3.1.2 Responding to Questions

Through analysing the opinions of the opponents, the spirit of the Convention and its specific provisions, it is clear that the Convention is not in fact characterised by an extremely broad criminalisation and does not ignore human rights, which are even guaranteed in both substance and procedure. The questioning of the excessive broadness of the criminalisation of the Convention has been expressed in two main ways, directly and indirectly.

Clarify Suspicions of Directly Extend the Scope of the Accusation. *The Convention* is not an extensive list of offences. The establishment of *the Convention*'s system of offences was one of the controversial issues throughout its formation and development, with each country expressing its own concerns on the basis of values, culture and actual national conditions, and thus proposing different offences to be included in *the Convention*. Taking internet pornography offences as an example, European countries are more open to adult pornography and focus their efforts on fighting against child pornography, while Iran treats adult pornography in the same way and believes that adult pornography also needs to be cracked down on (Zhang & Gong, 2020). On the whole, compared with the advocates of the narrow criminalisation pattern, the advocates of the broad criminalisation pattern believe that *the Convention* should include offences other than pure cybercrime, and at the same time take technological developments into consideration, trying to make up for the lag in law-making in a timely manner. However, compared with the text of the former sessions of the Special Committee, the final adopted text deleted 17 traditional cybercrime offences, such as copyright infringement. And in terms of the constituent elements of each offence, some of them have also been streamlined and lightened, such as article 14, paragraph 4, of *the Convention* on the determination of the exceptions to the child pornographic material (Jing, 2024; Li, 2025). It can be seen that *the Convention* does not show the characteristics of a broad criminalisation pattern, but rather favours a narrow criminalisation scheme. At the same time, the author believes that there is no basis in reality for criticising *the Convention* for being too broadly criminalised on the basis of the argument that it may be relied upon by some States to criminalise a wide range of offences at the domestic level. *The Convention* itself does not have the ability to directly intervene in domestic governance, and how to effectively and appropriately reconcile domestic and international law mainly lies at a country's own rule of law capacity and political strategy.

Dispelling the Suspicions of Indirectly Extend the Scope of the Accusation. It has been argued that *the Convention* is given a broad scope of application because article 3 of *the Convention* provides for the application of it to all stages of the prevention, investigation and prosecution of offences, while article 4 provides for the linking of *the Convention* with other United Nations conventions, such as *The Convention against Transnational Organized Crime*, by requiring States parties to incorporate into their domestic legal systems the action of using the Internet to commit those offences included in these Conventions (Wu, 2025). Thereby, this indirectly expands the offence system. In the author's view, this is not the case.

First, the phrase "applicable to all stages of the prevention, investigation and prosecution of offences" is a procedural safeguard, a means of ensuring that the spirit of law-making can be carried out and reflected in the entire process of prosecution, and has no substantive impact on the judgement of the broadness of criminalisation in substantive terms.

Secondly, the provisions of article 4 of *the Convention* on linkage with other conventions do not establish additional offences outside of those conventions, and a distinction needs to be made between offences and crimes in different jurisdictions, that is, whether or not new criminal offences are established in essence. To be more specific, the method in which an offence is "committed through information and communication technology systems" does not have the "resistance" which helps this offender escape from punishment according to the existing laws, even facilitates the perpetration. And even if the offence is not committed in that manner, the circumstances and consequences of the act are already worth punishing. Furthermore, paragraph 2 of the article stresses that "nothing in this article shall be construed as establishing a criminal offence in accordance with this Convention". It is clear that article 4 of *the Convention* is in fact a cautionary provision, which is intended to remind and stress the importance of not overlooking the special circumstances of the use of the Internet to commit an offence and to reiterate the specificity of the basic provisions. In addition, the view that the creation of a new provision is equivalent to the establishment of a completely new criminal offence is also too arbitrary. The offence is only a superficial judgement. The reason why some countries will create a new offence or article in such situation is that some of the provisions of *the Convention* can not be organically integrated into the existing domestic legal system, so, in order to better integrate with the treaty, they have to supplement or explain through these new articles. Therefore, in the light of the spirit of the purpose of *the Convention*, the author believes that articles 3 and 4 of *the Convention* do not encourage the establishment of a new criminal offence in accordance with a Convention other than the two conventions, which certainly does not lead to the alleged indirect expansion of the scope of criminalisation.

Human Rights Concerns of the Convention. During the negotiation process of *the Convention*, human rights issues were one of the focal points of the game in the draft treaty. While China, Russia and other countries have consistently emphasised national sovereignty over cyberspace, countries and regions led by the United States and Europe are more inclined to emphasise human rights protection. Under the impetus of Western countries, the current text of *the Convention* has a considerable degree of reflection of the concern for human rights protection (*Secrss*, 2024). Article 6 of *the Convention*, as an independent provision on respect for human rights, gives great human rights concern to the fight against cybercrime in the status of a fundamental principle, and paragraph 2 of this article also specifically lists the relevant obligations under international human rights law, such as freedom of expression, belief and association, so as to make clear *the Convention*'s value position of respect for and protection of human rights. The procedural safeguards set out in article 21, paragraph 2, of *the Convention*, the conditions and safeguards provided for in article 24, the protection of personal data in article 36, and the affirmation of the principle of non-discrimination in mutual legal assistance in article 40, paragraph 22, also reflect that *the Convention* has in fact affirmed the protection of human rights at the three levels of principle, substance and procedure.

3.2 Breaking the Ice: Combating Cybercrime as a Priority, Guaranteeing Human Rights Secondly

Although *the Convention* has textually balanced the scope of criminalisation and human rights guarantees, dispute is a subjective interpretation of objective rules, which may accompany *the Convention* all the way forward. In the future, with the continuous development of cybertechnology and changes in the international situation, *the Convention* still needs to be improved and adjusted to meet new challenges and needs.

3.2.1 Premise: The Need to Understand the Importance of Human Rights Guarantees

Human rights and cyberspace have grown so entwined as policy domains that comprehending one necessitates ongoing attention to the other (Aliyu, 2022). The controversy between the advocates of broad and narrow criminalisation patterns fully reflects the different considerations of human rights between the two sides. In order to find a compromise solution to the differences, it is necessary to clarify the necessity of human rights protection, so as to find the two protection thresholds at the opposite end of

the spectrum, and the two sides can then negotiate and consult within this reasonably closed scope. As we live in the same global village and participate in building a community with a shared future for mankind to meet various global challenges, the improvement and implementation of human rights protection also need to rely on the strategy of moving from domestic human rights concepts to international human rights concepts and finally to international human rights norms (Mao, 2023). How human rights are safeguarded in international exchanges reflects the international responsibility of each country and the value stance of its domestic governance.

International Responsibility. The establishment of the principle of the protection of basic human rights is the result of the joint efforts of the international community in recent times, reflecting the universal recognition of the human dignity and value of human beings. And as a basic principle of international law explicitly stipulated in international legal documents, different from jus cogens which mainly regulates treaty relations between countries, it is applied to all relations between countries. Respecting, protecting and fulfilling human rights is a responsibility and a right of all countries. The global governance of cybercrime should likewise insist on the implementation of the basic principle of protecting basic human rights, and should be integrated organically with other rules in order to build a just, prosperous and harmonious cyberworld.

Domestic Governance Requirements. When legal interests become the only object of protection of the law, the law loses its meaning of existence. The establishment of a society governed by the rule of law and the manifestation of the rule of law's spirit in the nation will be facilitated when citizens' fundamental rights are protected by coercive force at both the substantive and procedural levels. This will give them the confidence to express their desires and find legal solutions to their problems. At the same time, human rights, as a common value of all mankind, is an important foundation for building international trust, which, together with respect for national sovereignty, promotes equal democratic exchanges and cooperation among countries, providing an opportunity for absorbing and learning from each other's beneficial achievements. Governance practices vary from country to country, and the transnational nature of cybercrime has made the issue of how to govern it a hot topic of discussion in various circles; in the face of the problem of protection and punishment, human rights safeguards are a necessary consideration to ensure the legality and legitimacy of actions to combat cybercrime.

3.2.2 Path of Improvement

Adherence to the Fundamental Position of Combating Cybercrime. The primary purpose of the Convention is to strengthen the prevention of and the fight against cybercrime in a more efficient and effective manner. The mere pursuit of freedom and human rights in favour of an narrow criminalisation pattern is not conducive to the proper functioning of the Convention, while adhering to an overly broad criminalisation pattern in order to curb criminality harshly by blending the views of various countries will contribute to turning the law into an inefficient instrument of violence. And the ultimate result of both approaches is a departure from the original intent of each. Security is a prerequisite for human rights. Therefore, the author believes that the subsequent improvement of the Convention must insist the prior position of combating cybercrime while taking into account human rights protection to the greatest extent possible, rather than constructing a system of "human rights law" by sacrificing the essential, as draining the pond to get all the fish. Emphasis on human rights protection will dilute or even dissolve the purpose of the Convention in combating cybercrime (Secrss, 2024).

The Interface Between Domestic Law and Treaties. International treaties are essentially a coordination of wills between sovereign countries, and their effectiveness and governance effects ultimately depend on whether and how a country can coordinate the transformation and incorporation of international treaties so that they can live and work in peace and happiness at home. With the completion of the criminalisation system of the Convention, countries should update the relevant terminology in their domestic laws to ensure that the relevant connotations are consistent, complete and accurate, and integrate their domestic policies with the purposes of the Convention in order to improve the relevant domestic laws and regulations (Jing, 2024). The addition of provisions that do not yet exist in the country, as well as the path for their incorporation or transformation, should be carefully designed to ensure that the purpose of the legislation is not biased, that the constituent elements are appropriate and that the level of penalties is commensurate with the country's situation.

Creating a Bona Fide Research Exception Term. The Convention's provision on illegal access requires States to criminalise unauthorised access to computer systems, that is, it precludes the legitimacy of improvements such as testing systems. As computer security research is a key driver for improving cybersecurity, subsequent consideration could be taken to exclude certain acts that are bona fide and beneficial to the development of scientific and technological progress in the international community of mankind from the offences punishable under the Convention, so as to ensure the reasonable self-research and use of information by mankind. At the same time, in order to prevent some subjects from abusing this exception, an incrimination line can be set for the consequences of the act. When consequences exceed this line, the act should still be regarded as a crime, and a lighter penalty should be imposed than that for the act with subjective malice. However, the determination of good faith, the reasonableness of the judgement of the method, and the setting of the severity of the consequence will be a major problem that is worth discussing.

4 CONCLUSION

An analysis of the history of the discussion of the Convention and the specific provisions shows that the *Convention* has not, as most people believe, become a "pocket" full of cybercrime offences, and that the value of safeguarding human rights was reasonably taken into account by all parties in the conclusion of the Convention under the guidance of cracking down on cybercrime. However, the issue of human rights protection, as an important point of contention in the formulation and subsequent entry into force of the Convention, requires the joint efforts of all parties to resolve and negotiate a balance between different cultural value systems. In the author's view, under the stance of combating cybercrime while taking into account human rights safeguards to the greatest extent possible, it is possible to better reconcile the interests of all parties and promote international cooperation through such paths as better coordination of the *Convention* with domestic laws and setting up exceptions for bona fide research. This study rectifies the question of the Convention's overly broad criminalisation to suppress human rights, and proposes feasible paths to improve human rights guarantees by taking into account the reasonable concerns of all parties. So as to help more subjects understand the purpose of the *Convention*, eliminate relevant concerns, and actively participate in signing it, thus accelerating the effect of the Convention in combining the strengths of all countries to crack down on cybercrime and safeguard a wider range of human rights. However, as to how to carefully reconcile the *Convention* with domestic laws and introduce well-thought-out security exceptions in accordance with the actual situation of each country, a certain country may be determined to be the subject of future research to further deepen the understanding of this issue and explore the practicality of the programme.

REFERENCES

Albader, F. 2022. The pivotal role of international human rights law in defeating cybercrime: amid (un-backed) global treaty on cybercrime. *Vanderbilt Journal of Vanderbilt Journal of Transnational Law* 55(5): 1117-1144.

Aliyu, B. 2022. Examination of the constitutional and human rights issues in cyberspace. *Law and Social Justice Review* 3(3): 50-58.

Chalana, A. & Bhanu, A.P. 2024. Protection of human rights in cyberspace. *Jus Corpus Law Journal* 4(3): 646-656.

Jiang, S. 2023. New mechanism of international law for combating cybercrime. *Law Science* 2(1): 181-208.

Jing, L.J. 2024. Deficiencies and prospects of the "Criminalisation" part of the United Nations Convention against Cybercrime. *China Information Security* (8): 61-65.

Li, B.C. 2025. Review of the core issues of the United Nations Convention against Cybercrime. *Jurisprudence Forum* 40(1): 92-103.

Mao, J.X. 2023. The proliferation of international norms in Xi Jinping's important discourse on respecting and guaranteeing human rights. *Law Forum* 38(1): 16-26.

Secrss. 2024, November 8. Western countries challenge UN Convention against Cybercrime over human rights protection. https://www.secrss.com/articles/72180.

Tropina, T. 2024. "This is not a human rights convention!": the perils of overlooking human rights in the UN cybercrime treaty , *Journal of Cyber Policy 9*(2): 1-21.

Wu, S.K. 2025. The governance system of the United Nations Convention against Cybercrime and China's response. *China Law Review* (1):214-226.

Zhang, L.Y. & Gong, W.C. 2020. National positions on legal issues related to the United Nations Convention against Cybercrime. *China Information Security* (9): 85-88.