GEODE

Géopolitique de la Datasphère

UN Global Digital Compact

Submission by GEODE

April 2023

www.geode.science

ABOUT GEODE

The three coordinators for the submission are members of the GEODE Center. “GEODE” stands for Geopolitics of the Datasphere.

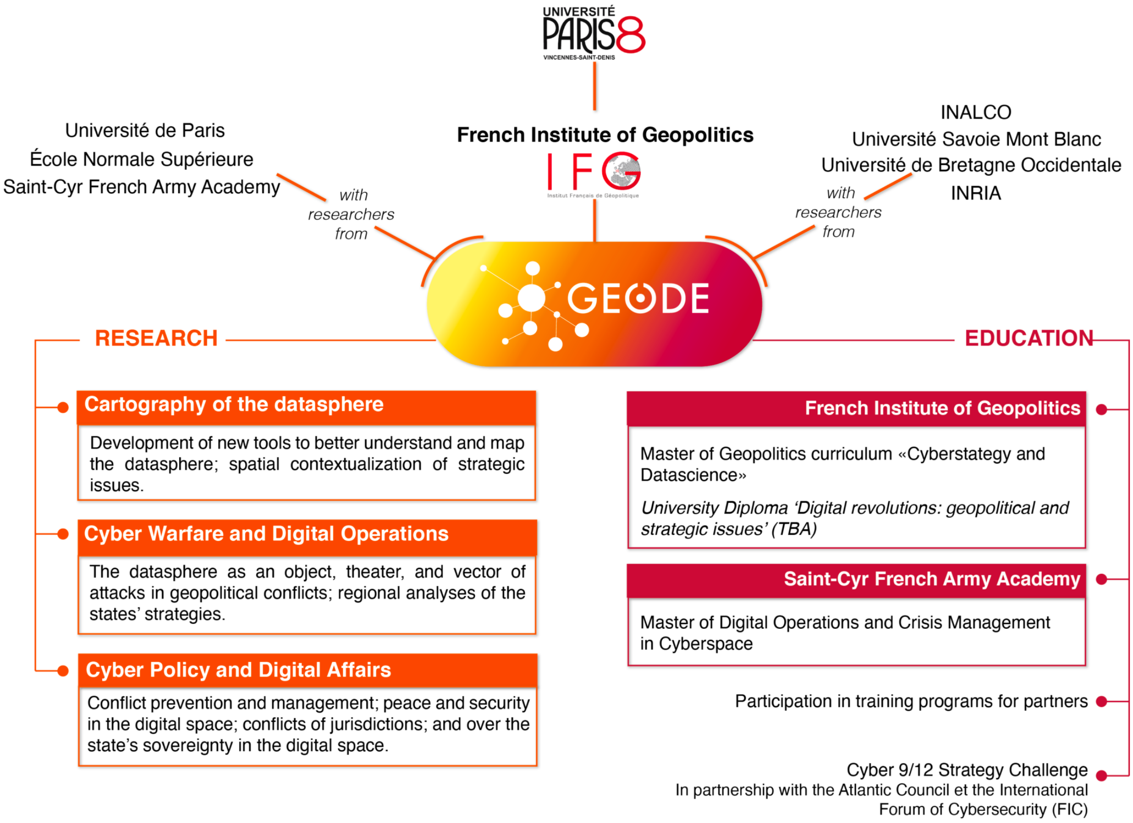
GEODE is a multidisciplinary research and training center dedicated to the analysis of strategic and geopolitical issues raised by the digital revolution. The Center is supported by the University of Paris 8 (France) and has been awarded the “Center of Excellence” label by the French Ministry of the Armed Forces as part of the Higher Education Pact. It is also the largest recipient of the William and Flora Hewlett Foundation’s Cyber Initiative program.

The emerging notion of Datasphere allows the analysis of strategic issues related to cyberspace but also to the geography of data flows and data control, the understanding of informational space, the mapping of topological networks, the fusion of geolocalized and non-spatialized data.

The scientific ambition of the researchers at GEODE is twofold.

On the one hand, the researchers use the resources of the datasphere for geopolitical analysis. In other words, they develop tools to collect, process and exploit the large masses of data relating to the datasphere. They also call for the development of new methods for mapping physical spaces based on the fusion of spatialized and non-spatialized data.

On the other hand, the researchers at GEODE study the datasphere as a geopolitical object in its own right, with an analysis of the defense and security issues that they cover, in order to feed a comprehensive strategic reflection that takes into account the strong entanglement of civil, industrial, and military issues. This objective includes the development of a specific cartography to better understand and represent the datasphere.



French Institute of Geopolitics

Université de Paris
École Normale Supérieure
Saint-Cyr French Army Academy

with researchers from

INALCO
Université Savoie Mont Blanc
Université de Bretagne Occidentale
INRIA

with researchers from

GEODE

RESEARCH

Cartography of the datasphere

Development of new tools to better understand and map the datasphere; spatial contextualization of strategic issues.

Cyber Warfare and Digital Operations

The datasphere as an object, theater, and vector of attacks in geopolitical conflicts; regional analyses of the states' strategies.

Cyber Policy and Digital Affairs

Conflict prevention and management; peace and security in the digital space; conflicts of jurisdictions; and over the state's sovereignty in the digital space.

EDUCATION

French Institute of Geopolitics

Master of Geopolitics curriculum «Cyberstategy and Datascience»

University Diploma 'Digital revolutions: geopolitical and strategic issues' (TBA)

Saint-Cyr French Army Academy

Master of Digital Operations and Crisis Management in Cyberspace

Participation in training programs for partners

Cyber 9/12 Strategy Challenge
In partnership with the Atlantic Council et the International Forum of Cybersecurity (FIC)

GEODE
Campus Condorcet
Bâtiment de recherche Nord
14, cours des Humanités
93322, Aubervilliers FRANCE

COORDINATORS

Aude GÉRY, Post-doctoral Researcher at GEODE, aude.gery02@univ-paris8.fr

Valère NDIOR, Law Professor, Université de Brest (France), Researcher at GEODE, Member of the Institut universitaire de France, ndior@univ-brest.fr

Anne-Thida NORODOM, Law Professor, Université Paris Cité (France), Researcher at GEODE, anne-thida.norodom@u-paris.fr

The opinions expressed in this text are the sole responsibility of the authors

EXECUTIVE SUMMARY

One of the popular beliefs about cyberspace, particularly from an international law point of view, is that it is a lawless space. This view is unwarranted despite the lack of a universal treaty regarding that matter. Undoubtedly, a **variety of international law instruments can be applied to cyberspace and to digital activities in general**. All the fields from international law should be leveraged to do so: international human rights law, international humanitarian law, international criminal law, international trade law, space law, etc.

Still, two caveats should be considered. First, due to challenging legal debates between States regarding the digital sector, many non-state initiatives have emerged to propose interpretations of international law, or even new standards. Second, the legal value of the hundreds of instruments that may apply to digital activities varies greatly.

Undoubtedly, the lack of an international treaty (notwithstanding the Council of Europe's Convention against Cybercrime) is one explanation for this large number of instruments and initiatives. Alongside the classic sources of international law (treaties, customary law, general principles of law), these instruments and initiatives have a varying normative scope, are seldom legally binding and range from simple reports and guidelines to unilateral acts or secondary legislation enacted by international organizations, including non-conventional concerted acts. Their vast majority cannot be relied upon to hold private or public digital actors responsible in the event of violation of their obligations.

While this variety of instruments and initiative contribute to providing a framework for digital activities, a clarification of the applicable law should be provided at an international level.

The emergence of new technologies has **profound political, social and economic implications**, both positive and negative, that should be addressed by international law. Several challenges and opportunities arise from the use of digital technologies: relationship between public and private actors, political instrumentalization of international law on digital issues (right of access to the Internet, content control, data protection) and endemic digital inequalities.

The adequacy of existing legal rules to address these challenges is constantly assessed in the light of the impact of new technological developments. Existing academic and policy discussions often debate whether current international legal rules are clear, precise and comprehensive enough to keep up with the rapid pace of digitalisation. It is no longer time to simply raise this question and reiterate the principle of the applicability of international law to cyberspace. It is now time to **provide concrete and operational answers that will meet the regulatory needs of the digital sector**.

In accordance with the principles of Internet governance recognised by the World Summit on the Information Society, non-state actors' views must be taken into account in the formation and application of law. Operational mechanisms that will enable effective multi-stakeholder and multilateral governance should be envisioned to enable balanced relationships between private and public actors. **Cooperation and co-regulation processes that include all stakeholders** should be fostered, rather than strictly dividing roles between public actors dealing with public policy and private actors dealing with technical issues.

TABLE OF CONTENT

Connect all people to the internet 1

Key commitments 1

Avoid internet fragmentation 1

Key commitments 2

Protect data 2

Key commitments 3

Apply human rights online 4

Key commitments 4

Accountability for discrimination and misleading content 5

Key commitments 5

Regulation of artificial intelligence 6

Key commitments 6

Digital commons as a global public / Good Internet governance 7

Key commitments 8

Connect all people to the internet

Restrictions to internet access can violate both international human rights law as well as treaty provisions related to the rule of law and democratic processes. While not specifically enshrined in the international legal instruments, the requirement that States should not interfere with people's access to the Internet can be addressed, among others, through freedom of expression and right to information safeguards.

To this end, internet restrictions should be considered not merely as technical measures affecting the logical or physical layers of the networks, but also as a tool used to impair the means of expression of individuals (see below, *Avoid internet fragmentation*). Therefore, internet shutdowns and content blocking may constitute violations of the principles contained in several international human rights instruments, in particular article 19 (right to freedom of expression, the scope of which is clarified by General Comment 34 of the Human Rights Committee) and article 21 (right of assembly) of the International Covenant on Civil and Political Rights (ICCPR). Regional conventions for the protection of human rights generally include similar provisions.

This perspective is supported by the practice of several organs and international institutions, notably resolutions adopted by the Human Rights Council on "The promotion, protection and fulfillment of human rights on the Internet" (A/HRC/32/L.20, June 27th, 2016). The Council condemns measures that seek to "*intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law, and calls upon all States to refrain from and cease such measures*", relying on a substantial number of secondary legislation not specifically related to the issue of Internet access. Several UN Special Rapporteurs have recognized the fundamental nature of the right of access to the Internet through the prism of freedom of expression or the right to peaceful assembly. However, this right of access to the internet should not be construed as a duty of States to provide access without any charge.

Key commitments

- *States should refrain from restricting people's access to the internet, in order to comply with relevant human rights instruments.*

- *States should recognize that access to the internet is a driver for development and must be safeguarded.*

Avoid internet fragmentation

Since the early 2010s, several States have introduced policies that prevent their citizens from accessing a global and open Internet. Some of them have even gone as far as trying to demarcate their digital space, creating borders of a sort through the development of dedicated domestic infrastructures and, thus, isolating themselves more or less from the rest of the digital universe. Other States resort to data relocation processes, with the aim of making it a condition for digital companies to continue their activities that data be processed on their territory.

Cybersecurity issues, disinformation, data breaches, personal data protection and national security requirements have been used as justifications to create *de facto* intranets.

This results in an "internet fragmentation" (or internet segmentation), in other terms the creation of a technical border around their territory, ranging from the discrimination of certain categories of information to the complete blocking of data flows to and from the outside world. As a result, internet users from a specific country may be totally prevented from interacting with users based abroad and may be unable to access certain content, websites or applications.

Internet fragmentation should not only be seen as a set of technical measures that create borders within the logical or physical layers of the networks. In most cases, it will also restrict the means of communication of individuals, and thus their capacity to meet, consult, mobilize, inform and be informed at a global scale. Internet fragmentation notably includes creating bans on global social media platforms or search engines with the intent to prevent citizens from accessing content that is of vital interest to them and may help them keep informed. This type of measure can be a way for governments to control the digital activities carried out "on" their territory, to isolate their country from the rest of the network and even to create blackout situations for populations in the case of internet shutdowns. Users often use VPNs to bypass these restrictions. However, such practices have been deemed unlawful by several legislations across the globe, in order to discourage them, while most users are unaware of how to safely use VPNs.

Thus, internet fragmentation is harmful from the point of view of international human rights. It can be an indirect way of restricting individuals' digital activities and violating principles set out in several international instruments.

Key commitments

- *States should promote a global, open and neutral internet.*
- *Security issues should not be used as a pretext to infringe on human rights by limiting users' access to global content.*
- *Companies should be encouraged no to contribute to internet fragmentation.*

Protect data

Digital data has become an inescapable resource that raises contradictory issues: protection of human rights and privacy, national security, economic development, data circulation, digital sovereignty, application of the law to the multiple uses of data, etc. The increase in the volume of data and the diversification of its uses, in particular with artificial intelligence (AI), raises new questions in terms of governance of this data.

The interpretation of privacy provisions will be of particular importance in the future, because it is a fundamental right and one of the elements of the legal regime for the protection of personal data. This right is at the heart of complex situations such as mass and targeted surveillance by public and private actors, interception and storage of personal data to fight cybercrime, extraterritoriality of data protection regimes, and principles framing this protection (right to be forgotten, right to rectification, principle of consent to the processing of one's personal data, purpose limitation, data minimisation, accuracy, lawfulness, transparency, lawfulness, data storage limitation, confidentiality and integrity, etc.).

The diversification of data implies a better identification of the types of existing data to adapt the regulation of their use. For instance, one may wonder if digital data is an asset under international humanitarian law during armed conflict, international trade law or in the law of diplomatic immunities.

Since an international legal regime is currently lacking, there is a tendency to adopt laws at regional, national or even sub-national level, which include provisions with extraterritorial scope. This increases the risk of conflict of laws and creates difficulties, particularly in cross-border data flows and mutual legal assistance.

Collecting, sharing and selling digital data, in particular personal data, has both positive and negative human rights implications. Practices such as targeted advertising, content monitoring, private and public surveillance, spying, data collection for criminal investigations, internet filtering, use of biometric data, etc. can endanger privacy and freedom of expression. But digital data and AI can also contribute to improving the human condition. Thus, it is necessary to steer regulation towards a virtuous use of data.

Key commitments

- *Data should be defined and categorized more precisely (personal data, sensitive data, security data, etc.) to adapt their legal regime according to their nature and use. Many efforts have been made in the field of personal data protection but many other data should also be regulated.*

- *With regard to personal data, the principles set out in the GDPR offer standards of protection which could be extended internationally to facilitate the circulation of data while preserving the protection of individuals. However, the interpretation of these standards needs to be harmonized in order to avoid conflicts of extraterritorial laws and regulatory fragmentation.*

- *In view of the evolution of the uses of data, whether for commercial or surveillance purposes, by private or public actors, the personal data protection regime should be refocused on the protection of privacy, which is its foundation, and no longer be developed as an autonomous regime, whose existence would be justified solely for commercial or security purposes.*

- *It is important to limit the risks of conflicts of law resulting from the extraterritorial scope of national laws by developing standards or even rules of international law.*

- *Data protection regimes should be developed to improve the human condition, reduce the digital divide, and facilitate the achievement of the SDGs.*

Apply human rights online

Digital activities should not be implemented without taking into account their impact on human rights, the rule of law and the democratic values enshrined in the UN Charter and related legal instruments. Business innovation concerns should be matched with the systematic use of impact assessments and critical risk assessments when developing technological tools and digital processes that may infringe on human rights. Similarly, national security concerns or public order considerations should not justify disproportionate infringements on individual rights.

To date, there is no specific framework for digital activities that is truly universal in scope, covering, for example, the protection of personal data, automated decision-making processes or online expression. The lack of a unique framework is likely to be leveraged by some States in order to exploit digital tools for the purpose of monitoring individuals and restricting their rights. Yet, despite the lack of a universal digital-specific instrument, resorting to pre-existing legal instruments is a reliable way to protect individuals and community's rights in the digital sphere.

Indeed, in practice, a majority of United Nations Member States recognize the application of pre-existing rules of international law in the digital sphere, including those derived from international law instruments (United Nations Charter, International Covenants of 1966, regional charters for the protection of human rights, etc.). International human rights law is the most obvious and most visible way of addressing practices on the Internet, whether it be to regulate the activities of public actors (States, local authorities, international organizations) or those of private actors (companies, non-profit organizations). The reassertion of the States' positive obligations in this respect appears particularly necessary in the face of the infringements caused by private actors.

In this respect, it would seem vital for the international community to recognize that human rights, as enshrined in the relevant legal instruments, apply in the digital sphere, particularly online. The statements of actors refuting this vision are at odds with the actual practice, including international and regional case law.

Key commitments

- *States should recognize that human rights, as enshrined in the relevant legal instruments, apply in the digital sphere.*
- *Impact assessments processes and critical risk assessments should be implemented when developing technological tools and digital processes that may infringe on human rights.*
- *States should refrain from restricting individuals' legitimate access to technological tools.*

Accountability for discrimination and misleading content

Digital platforms are, at the same time, spaces for the promotion of human rights and democratic processes and the tools that may lead to their erosion.

Initially, these platforms were mostly recreational or informative in nature. Over time, they have acquired a critical role as spaces for the civil society to mobilize or to expose regimes that do not respect fundamental rights. Today, they have become an indispensable tool for almost half of mankind: close to three billion individuals use the services offered by tech companies, most notably social media. However, the continuous stream of content published by users generates numerous abuses that can only be addressed by moderation mechanisms (deleting content, marking it, downgrading it or evicting users). Discriminatory comments, calls to hatred or violence, defamation, privacy breaches or disinformation operations are among the harmful behaviors that platforms have to regulate in real time.

However, acting against unlawful content comes with challenges. The first is that content moderation is carried out by companies on the basis of specific standards that do not always comply with laws and regulations, particularly in terms of human rights, and that are applied on an international scale without adapting to local cultural contexts. The second is that, when it is not automated, the moderation activity is entrusted to employees or subcontractors who may be based in remote regions of the world and who are generally ill-equipped to determine when content is legitimate or not.

These two factors can lead to zealous or hasty moderation practices, likely to constitute an infringement of freedom of expression. On the other hand, some content that should be moderated because it violates human rights or undermines public order or democratic processes remains online as a result of commercial decisions. States should take the necessary measures, in accordance with international law, to oversee the moderation activities of platforms and make them accountable. It is essential that content violating fundamental rights be treated according to due diligence standards and that freedom of expression not be subject to disproportionate restrictions.

Key commitments

- *States should* address *disinformation and misinformation practices in coordination with companies, civil society and users.*

- *States should take the necessary measures, in accordance with international law and their national laws, to oversee the moderation activities of platforms and make them accountable for their shortcomings.*

- *Online moderation policies should always be interpreted and implemented by companies and State actors in accordance with relevant international human rights instruments.*

- *States should not misuse the prevention of disinformation as a pretext for disproportionate restrictions on freedom of expression*

Regulation of artificial intelligence

No longer only embedded in products and industrial systems, artificial intelligence (AI) has recently made a breakthrough in our everyday life through becoming accessible and directly usable by end-users. In doing so, computing power and algorithms are more than ever processes and tools that are impacting our lives, our economies and our democracies. AI can bring innovation and progress for individuals and democracy, by offering new modes of expression and production. Considering the global challenges that our societies are facing, AI provides new means to address them, particularly in the domains of public health and the environment. AI-based products and services can also play a role in strengthening the rule of law and the enforcement of international law, including through monitoring and evaluating the implementation of States' international commitments.

However, the development of AI is not without risks to the fundamental rights and freedoms of individuals, the rule of law, and international development. Indeed, AI learning models require large volumes of data, which process can disregard the legal protection attached to the data. Biases from data processing are multiplied, creating new and often underestimated risks of discrimination. In a context where non-state actors, especially companies, are the main holders of this data, the under-representation of certain regions of the world and the concentration of capacities in the hands of a few actors present a risk for cultural and social diversity and international development. Thus AI contributes to the reinforcement of the digital divide and the confinement of the individual through the prism of data. Finally, because of its very operating processes, the impact of AI on the environment is becoming a major issue that remains unevaluated.

The multiplicity of AI uses undeniably constitutes a difficulty when tackling its regulation. The unknowns accompanying its consequences on societies and fundamental rights must be seen as alerts guiding each step of the development of a technology, a product or a service based on AI. The open sourcing of AI systems and the conditions for their reuse should be given particular attention in order to encourage development that is consistent with international law, and in particular international human rights law. As such, AI thus constitutes a new area in which States' positive human rights obligations find their way, and in a potentially new dimension.

In recent years, numerous normative initiatives have emerged to regulate the development and use of AI. They tend to set a minimum of commitments for AI, regardless of sector-specific needs. Yet, sectoral approaches might be needed to better tackle the challenges. Similarly, an autonomous approach to AI should not lead to its omission from forums dealing with other subjects, notably cybersecurity and the environment. In both cases, the ethical approach is not sufficient in itself. It is also interesting to note that despite an ethical approach to AI regulation, the content of the instruments discussed is often very legal. The choice of legal over ethical should be preserved.

Key commitments

- *Any development of an AI product or service should only be conducted after a careful risk assessment and should be compatible with human rights frameworks. In case of high or undetermined risks for human rights, the development of an AI product or service should be prohibited or only conducted under high scrutiny from public authorities.*

- *States should set up independent authorities tasked with overseeing the development and uses of AI by state and non-state authorities. Those authorities should be given appropriate means and resources. They should not exclude the recourse to judicial authorities in case rights and obligations are being abused.*
- *Next to the international consensus on accountability, responsibility and transparency as core principles guiding the development and use of AI, States and non-state actors should cooperate on the concrete implementation of these principles through the exchange of best practices in order to engage in more precise regulation.*
- *Independent research on the biases and negative impact of AI technologies and services should be conducted. State and non-state actors should thus cooperate with researchers to develop evidence-based research.*

Digital commons as a global public / Good Internet governance

As early as the World Summit on the Information Society in Geneva and Tunis (2003 and 2005), stakeholders called for multilateral and multi-stakeholder governance. These governance modalities have constantly been called for (Net Mundial Declaration, São Paulo, 2014; UNGGE and United Nations OEWG reports on international cybersecurity) but have not, however, made it possible to respond to the challenges of the digital era or to prevent deadlocks in international negotiations.

The issues at stake in international negotiations are essentially geopolitical but also have a legal impact. States are competing to impose different conceptions of Internet governance: some of them see the digital sphere as an essentially economic opportunity, some focus on human development and others give priority to state security. These conflicting conceptions hinder the application and adaptation of international law to digital activities. The geopolitical challenges surrounding Internet governance also affect the model of cyberspace itself, contributing to its fragmentation, the integration or non-integration of infrastructures, the inclusion or exclusion of the informational dimension. Internet governance depends on the way in which the Internet and, more generally, the digital object are described: critical infrastructure, global risk, common good. Each of these qualifications entails the application of a particular legal regime and the involvement of specific governance actors. Thinking of the Internet as a common good requires us to consider the global management of its resources, namely data, on the model of the International Seabed Authority, for example. But unlike other international regimes for managing the commons, the resources constituted by digital data are not limited; on the contrary, they are growing exponentially. Existing regimes must therefore be adapted to the specificities of digital data.

The consequences of these conceptual oppositions are manifold: States cannot reach a consensus on what good governance should be to ensure the security and stability of cyberspace; the logic of coalition between certain States is reinforced, contributing to a greater fragmentation of regulation and the exclusion of certain States from the scope of the discussion; certain issues, such as cybersecurity, cannot be settled or are settled in a roundabout way from an economic angle, for example (see the OECD's work on this point).

Key commitments

- *Strengthen multilateralism by including developing States and by promoting dialogue between the different conceptions of cyberspace and applicable international law.*

- *Implementing in a more concrete way multistakeholderism through the notion of co-regulation: the balance between stakeholders is not necessarily the same according to the subjects to be regulated; the modalities of cooperation between public and private actors may vary according to the fields of action.*

- *Encourage cooperation between international institutions dealing with Internet governance to avoid regulatory fragmentation. Current governance tends to distinguish between subjects and bodies, whereas these subjects (technical or political) are increasingly intertwined. Cooperation mechanisms between the institutions (public, private, hybrid) concerned must be established.*