

The Digital State's Sovereignty: the Algerian approach

السيادة الرقمية للدولة : المقاربة الجزائرية

Naili Habiba

University of Algiers 1, Faculty of Law

Laboratory of Mechanisms for achieving

Integrated Development in Algeria

h.naili@univ-alger.dz

Date of submission:10/04/2025 Date of final acceptance:17/09/2025 Date of publication :September

Abstract :

Sovereignty's erosion and decay phenomenon has been observed for years by legal philosophers who called politicians and decision makers for remedy, as the situation has escalated in reason of the digital sphere's lawless spreading out.

The international awareness of the danger cyber-crimes over digital sovereignty needs a responsible international community position, sharing the same values about national security. However, expansionist intentions took over some powerful countries common sense, to divert the use of digital tools as lethal weapons.

At that point, rational nation-states privileged the defensive approach, under cover of international law, prevailing respect of State's sovereignty over its whole territory even digital space and frontiers. Algeria, as unwavering peacemaker country preferred the defensive doctrine associated to digital empowerment, by strengthening its legal arsenal and institutional actors.

Keywords : sovereignty, digital space, state , Algeria, defensive doctrine

ملخص:

إن ظاهرة تآكل السيادة و انكشافها تم ملاحظتها منذ سنوات من طرف فلاسفة القانون الذين نادوا رجال السياسة و صناع القرار لمعالجتها، خاصة في ظل تفاقم المسألة بسبب التوسع غير المسبوق للفضاء الرقمي خارج إطار القانون. الوعي العالمي حول خطورة الاجرام السيبراني على السيادة الرقمية يتطلب موقفا حازما للمجتمع الدولي الذي يتقاسم نفس قيم الامن القومي، لكن النوايا التوسعية لبعض الدول القوية فاقت حكمتها، فحوّلت استعمال الادوات الرقمية لأسلحة فتاكة.

لهذا، فضلت الدول ذات الفكر العقلاني تبني مقاربة دفاعية تحت غطاء القانون الدولي الذي يقدم و ينادي باحترام السيادة الوطنية و بسطها على كل اقليم الدول حتى الرقمي منه. والجزائر كدولة مسؤولة ومبادرة للسلام، فضلت تكريس العقيدة الدفاعية مع تدعيم ترسانتها القانونية و المؤسساتية.

الكلمات المفتاحية: السيادة؛ الفضاء الرقمي، الدولة، الجزائر، العقيدة الدفاعية

Introduction:

The state's sovereignty is the ability to perform internal governance and normative production but also the capacity to run foreign affairs as peer-to-peer State.

This concept remained for the few last centuries, a critical point in scientific, scholar and political debates because of its immaterial characteristic compared with the classical and tangible elements of the state such as the territory, the population and the political authority or even international recognition.

The Westphalian historical background of the sovereignty's definition hardly survived the modern geopolitical transformations, so a certain form of erosion stroked the concept and triggered its decay.

However, the post-modern era came along with new defies contesting the old perception of frontiers, transforming the world into a small village. It created a cyber-immaterial huge sphere connecting the entire world and escaping from all kind of rules or laws.

Indeed, the old world countries are more flexible and open-minded with cyber sphere and immaterial exchanges and even digital currencies, but for the third world countries often newly independent, old colonialist fears surface.

The question asked and discussed by this study is: **How are modern countries apprehending cyberspace to impose their sovereignty over it, and what is the particularity of the Algerian approach?**

Many **hypothesis** can represent obvious answers to that complex question, but it is worthy to study thoroughly the hidden side of post-modern perception of State-sovereignty through those suppositions.

Then, it could be interesting to proceed almost by elimination, and explain each of them starting with the less probable to the most plausible, as following:

- First hypothesis, we can suppose that sovereignty's erosion phenomenon is a fatality and globalisation era made it worse,
- Second hypothesis, we can hope that sovereignty is going through a conceptual revolution to make it live again and progress,
- Third hypothesis, we can be realistic to enhance the scientific debate and feed it with the fact that great countries are trying to take over cyber-space, leaving the others behind, which makes a promising growing country like Algeria to consider a pacific but not naïve approach.

The growing awareness in sovereignty as an element to frame and to reflect on digitization has become the subject of a number of recent review articles (Couture & Toupin, 2019; Hummel et al., 2021) and discussion pieces (Glasze et al., 2022; Pohle & Thiel, 2020).

These studies came up with specific perceptions of the impact of digital technologies and environments and their impact on classical definition of sovereignty.

However, this paper approaches the dilemma through a new understanding, using comparative and descriptive methodology; starting with investigating the conceptual decline of State sovereignty (**Section I**) then the eternal hegemony race of the greatest countries to take advantage of the offensive potential of cyber-space (**Section II**) to end with the Algerian defensive and peaceful efforts to contain the imminent danger (**Section III**).

Section I: The conceptual decline of state sovereignty: truth or convenient myth?

The classical pillars and dogmas of constitutional law, such as nation-states or incontestable State sovereignty in the decision making process, are increasingly questioned in reason of globalization and the ascending power of non-State actors.

The new world order seeking allegedly for peace, introduced a new supra-national system of rules and laws especially for facilitating and smoothing international trade and protecting investments.

Unfortunately, nation-states have been overwhelmed by the huge flood, and were obliged most of the time to agree with conceding a part of their sovereignty, to save their “chairs” in international community forum.

Scholars called that political and normative phenomenon, the erosion of State-sovereignty because of the fragmentation of norm-making power between classical actors and improbable ones **(A)**.

Unexpectedly, once the idea of sovereignty’s decay was established, the cyber space emergence as an imposing new factor revives the debate.

Indeed, the digital tremendous sphere engenders states’ interest by considering it as the fifth dimension of sovereignty in order to set control over it **(B)**

A). Sovereignty erosion phenomenon

The history of modern State is the expression of scholars’ thoughts battle, devoted to build strongly the concept of sovereignty as impersonal power to recognize the representative and public character of the Office.

The concept progressed through a double dynamic, requiring inside centralisation revealed as absolute power over a territory and a sedentary population.

The second movement involved a power centralisation toward the outside, emancipating State power from church hegemony and from embodied power perception of sovereignty, to reach the institutional authority.

Indeed, the medieval State power was considered as monarchs’ ownership, sacred and protected by Church; and court philosophers like **Hobbs** who pleaded for absolute power and loyalty to the King, or **Rousseau** presuming people’s good will to obey and respect the “social contract”.¹

However, Church’s manipulations and kings’ misbehaviours provoked popular revolutions lead in France on 1789 by great revolutionaries like the controversial figure **Robespierre**, and consequently a new era started for modern power practice; at the opposite of embodied form of power; then, sovereignty became citizens’ undivided property.²

Major controversies remained to a certain extent, until the accomplishment of full transition to the institutionalized form of power, enriched by foremost principals such as democracy, fair elections, separation of powers and hierarchy of norms.

The State normative edifice was conceived to be strong and delightfully decorated with philosophers’ idioms on liberty, equity and people’s well-being.

At last, clear frontiers were drawn according to the importance of public affairs’ protection and common interest scarcity; in order to justify State action with all due respect to citizen’s fundamental rights.

The French philosopher **Leon DUGUIT** predicted that the continuous evolution of modern societies leading to strengthen sovereignty empowerment process will, at certain point, be damaged and replaced by new dogmas³.

But during those last years, a paradigm-shift stroke public law, stating that law should be conceived as normative rule of conduct deriving strength and power directly from its own moral properties independently from State sovereign authority⁴.

This idea came along from globalization's vicious effects, prioritizing capital flows, international trade facilitation, communication networks, standardization of global purchasing habits; using social media influence, and more likely the emergence of supra-national regulatory system.

The fast growing of this phenomenon overwhelms country -states legitimate control and represent a greedy challenger affecting their capacity to regulate their markets and consumers' behaviour according to their own priorities and public policies⁵.

However, sovereignty will remain the expression of autonomy of the political domain, strongly attached to the juristic concept of State⁶.

Sovereignty, as common meaning, refers to the government's supreme control of affairs within a territorial or geographical area or limit. However, its determination has always been a matter of diplomatic dispute or even terrific wars.

The survival of that confident speech depends on the Stats' capacity of settlement and smart compromising with those new strong actors and normative competitors, by conceding the smallest part possible of sovereignty in order to keep safe the biggest part left.

Certainly, it is a flexible and realistic approach, which should be supervised and reinforced continuously by the international cooperation with other nation-States sharing the same values; rather than choosing the isolation solution almost impossible to consider at that point.

Moreover, when the new cyber sphere's threats woke up international sceptical countries, the highest level of awareness was required by international community as a unified entity with all divergences apart, to find out the adequate solution to neutralize that menace.

Thus, the perfect ally is to call back the ancient version of sovereignty and seek for every country's contribution to get over the globalization's fatality.

For the Algerian **constitution**, "The sovereignty of the State shall extend to its territory, airspace and territorial waters. The State shall also exercise its sovereign right, established by international law, over each of its different zones of maritime space belonging to it."⁷ Moreover, "it shall be emphatically prohibited to relinquish or forsake any part of the national territory"⁸.

The simple comprehension of that strong statement confirms the firm position of the Algerian doctrine regarding its sovereignty over all its elements even if the concept is enlarged to new dimensions, and the unfeasibility to consider conceding a single part of it.

It is known as the intangible principles of the constitution⁹, which are almost impossible to amend or change in due respect to liberation revolution and independence on 1962, because Algerian people are the real source of State power, resolved to sustain national sovereignty and freedom.

This type of articles comply with the statement of the article **223** concerning constitution's modification. Therefore, no amendment shall undermine for instance the republican character of the

State or the integrity and unity of the national territory; it represents a permanent exception to the possibility of the constitution's revision.

Undeniably, the Algerian approach regarding its sovereignty over cyber-space, benefits of the highest priority, since its considered part of the whole meaning of the national sphere, so any threat can be considered as act of war requiring strong respond.

B).The cyber space as fifth dimension of sovereignty

Country States are nowadays facing the fear of the unrestrained growing of cyber space, especially that their own citizens start feeling the danger of losing control over their personal data, ideas and innovations.

Indeed, the quintessence of sovereignty is the normative ability and the legitimate power to create the law and enforce it.

This incontestable power in "real world" is dangerously jeopardized and teased in the immaterial world; which remain a random variable most of the time, particularly in the disturbing dark web invisible sphere.

In fine, the greatest and most powerful States all over the world preferred to recognize the cyber space as a new or a fifth dimension accomplishing their sovereignty instead of disregarding it.

In legal terms, and for doctrinal pure purposes, this challenge can be considered as a "renaissance" for the declining concept of national sovereignty facing States' economic and political unions or greedy and rebellious multinationals.

As soon as cyber-attacks stroke, the old reflex of national law and sovereignty reappeared as perfect argument and articulate lawyer to preserve national security and vital interests.

The difficulty remains in determining the "cyber-frontiers" in order to identify the new dimension of sovereignty and normatively protect it, expecting huge complications if we compare that issue with land border determination for instance.

However, the actual claims for digital sovereignty assume that the intensive uncontrolled activity in cyber-space became more than worrying and disturbing and even tensions' raising with the rights and interests of the population concerned.¹⁰

Indeed, digital sovereignty recognition can generate many concrete consequences, like the fact that imposing authority over data free flows, does not obey to the old perception of geospatial constrained domain.

The difficulty of that mission increases by the fast advance of the technology and security breaches; so, as soon as an aspect is controlled or familiar to legislature, a new practice came up and creates a supplementary need for normative intervention.

As first step, States can cautiously initiate a control regulation over data access and sharing; by setting laws and binding rules determining with precision the quality of persons who can be let in governmental data bases or massive servers and defining a clearance highly secured system as breaches proof as possible and available.

This kind of frontiers is recognized and legitimately protected by different forms of passwords and fire-walls and many other means provided by anti-hacking well reputed programs.

In Algeria, specific set of laws distinguished three kind of data access ability, starting from the white information available for everyone, then more restrained grey information and at last the black information meaning that it is top-secret information forbidden to access, use or spread.

Section II: The sovereignty over cyber space: offensive doctrines

Once the cyber space threats measured and recognized, great countries, smaller entities or even individuals pursued the benefits of that huge harmful power.

Sadly, the offensive approach characterizes the strategy of the own defence and security for some States, because, they consider it as a dissuasive powerful method to keep up with foreign threats.

Great and powerful countries are performing their everlasting race using this new lethal weapon, sometimes by direct attacks but many other times by influencing opinions and creating new cyber-society networks **(A)**.

In fact, it became a dangerous mean for “bulling” and compromising authentic civilizations trying to save and hold onto their cultures from the globalization’s deleting and standardizing effect.

That’s why international community should intervene to protect global peace from both sides of the offensive acts performed in cyber-space against the prosper growing of humanity, by respecting the right of the other to exist and to be different **(B)**

A).The soft power and hard power cyber challenges:

The offensive tactic in cyber sphere has been initiated many years ago, and used to remote or paralyse enemy countries’ networks and energy stations representing a new figure of proxy wars.

Unexpectedly, the first data theft incident goes back to 1834 when two offenders stole financial market information from the French telegram institution. Since that, similar practices emerged to disturb phone service or wireless telegraphy.¹¹

But the title of first known hacker goes to **René Carmille**, considered as ethical hacker because he mislead German occupation army to help French resistant.

It can be considered as a primitive form of “**hacktivism**” performed nowadays by highly skilled hackers to make a point concerning a noble cause they defend.

However, the first cybercriminal is **Kevin Mitnick** who performed networks’ unauthorized access from 1970 to 1995, arrested by the FBI and becoming after prison a celebrated consultant.

In 1988, world’s networks knew the “Morris Worm” created by **Robert Morris** as a dangerous replicating virus launched, as he claimed, to measure the cyber-space size.

The democratization of high technology devices has definitely its part of responsibility of digital vulnerability, for instance, on 1999 a teenager could get inside the US department of Defense’s computers and damage their servers.

One year later, a Canadian high school student managed to compromise huge multinational’s databases like Amazon and e-Bay.

Then, the concept of **cyber warfare** emerged which implicates transforming hacking skills into weapons and declaring the offensive use of digital arms.

It officially begun on 2010 with the American attack setting of the **Stuxnet** operation targeting Iranian centrifuges used in uranium enrichment for the supposed nuclear program¹².

And between 2014 and 2016, **Russia** massively used strategic attacks against the German parliament and the State of Ukraine.

China also hijacked the American office of personnel management to steal employee's records and personal information.

Those edifying examples shows that great countries were dangerously fascinated by the power of digital "clean" wars, but once the danger came from unknown enemy like terrorist organization using data stealing for ransoms, a wiser course of action took over.

The offensive approach is certainly attractive but its consequences are more dangerous, especially at the artificial intelligence rising era.

In addition, the soft side of that power can be more harmful to states' stability; indeed, social media and applications used at the beginning for personal or professional networking and advertising, became recently an uncontrolled space for spreading fake news and destructive trending.

Each individual became citizen of the world and could communicate with anybody in the globe with no restrictions.

Nevertheless, the dream became quickly a nightmare full of disturbing behaviors and defamation, particularly confusing and dangerous for young users, first victims of brainless influencers and online gamers making some of them commit suicide.

Unfortunately, algorithms "ethics" to filter bad behaviours are insufficient most of the time and considered inconvenient to conservative society's cultures and morals.

At that critical point, some countries decided to block and ban some of those web sites or mobile apps impossible to control especially when it was established that their confidentiality policies are doubtful and dangerous to personal users' data.

For instance, the extreme example is **North Korean** regime restricting and controlling any simple use of internet; **China** decided also to ban social networks, spreading hate speech and calls for chaos.¹³

It seems that the fear of an experience like the Arab spring took over any beneficial outcome from social media, and prohibition remains the ultimate solution.

However, prohibitions generate most of the time an opposite to expectations result, because people become more interested to discover hidden information.

Therefore, the complexity of the question necessitates a significant global awareness and a strong and responsible position starting with greater countries charmed at the beginning by the potential of cyber space in their expansionist policies.

International serious collaboration is the key to take down the global common enemy and contain the damages already caused by its uncontrolled ascending.

But the old doctrinal dilemma and scholars debate reveals itself at that point, because international law has been always considered as the enemy of accomplished sovereignty, based on the necessity to give in external sovereignty, in order to obey a supra-state conventional mechanism of self-restrain.

This ancient enemy must turn into an actual friend, able to gather international community around a common target and face a universal threat; using data sharing and security cooperation framed by legal instrument as international treaties and conventions.

The enforcement of this soft-law once signed, depends on each country's commitment and seriousness to find out suitable and sustainable solutions to take advantage of this situation and neutralize its harmful effect.

B).The international law vs. cyber threats:

In reason of cyber-crime fast proliferation, the misuse of internet became available without requiring any particular skills¹⁴. Hackers offer their services on the dark web to blackmail or hijack individuals' personal data or even entire countries and governments; so they penetrate networks, possess top-secret data and annihilate them.

Famous hackers once arrested, American authorities often negotiate with them the possibility to be recruited to bust other hackers on the run. Reality or myth, but the idea that governments became obliged to settle with criminals, demonstrates the huge dimension of the problem.

Digital attacks are transnational and no geographical borders can limit them, unlike conventional attacks. That is the main reason for modern countries' motivation to recover their full sovereignty over their digital borders.

Globalization imposed the digitalization of countries management of public and private services, trade and economics, communication and transportations, in order to improve and facilitate people's life and accomplish their well-being¹⁵.

Nevertheless, the governance of cyber-space needs the intervention of international law able to structure relations among States and other international stakeholders or non-state actors, according to common rules and shared standards¹⁶.

Indeed, international law gained prominence, and thanks to State's increasing commitment representing a universal consensus on its applicability over the digital sphere, international treaties were born such as the **Budapest Convention** on Cyber-crime.

The convention was signed in Hungary on 23 November 2001 by the Council of Europe and other States, and it is considered all over the world as the main legal reference dealing with cyber-crimes proliferation.

At a continental level, we can refer to **African Union Convention** on cyber-security and personal data protection signed on June 27th, 2014, Algeria for its part signed and ratified the convention of **Malabo** (equatorial Guinea) on 2018 to consolidate the African position¹⁷.

And at the regional level, Algeria signed the **Arab convention against cyber-criminality** of December 21, 2010 ratified by **presidential decree 14-252** of September 8th, 2014

Digital technology is actually fast and dynamic, but at the meantime, more actors are joining the international community's movement to contain cyber threat through legal channels.

Therefore, the resistant to international law's instrument did not come from States or international organizations but from private actors and cyber-markets lobbies.

Any regulation of digital activity is considered as unjustified and unacceptable menace to free access to information, communication and freelance.

Indeed, international law is obviously unwelcomed and raises several issues as the unbinding general character of soft law, counting on the good will of its signing countries to translate its recommendations into actual laws.

In addition, existential disagreements and extreme differences in States' position toward digital threats remain obvious; some are offensive and opportunity takers when others are wisely defensive and peaceful.

Then, interpretative questions can occur especially when a country-state try to translate into practical measures a convention's general recommendations, and even inside public opinion and powerful actors can intervene in order to save their commercial interests.

Unfortunately, international conventions have limited attribution to recommend soft regulations to states and other recognized actors of international community; and even no competence to address directives to non-states and other random actors.

All those remarks refer to an accountability important concern; because if a State is accused by another State of practicing cyber misbehavior, it cannot easily be held responsible by invoking an international Convention or treaty.

At this point of divergence, a simple idea comes along encouraging an inclusive process, which associate every digital actor, to find out a common ground facilitating a constructive debate.

Section III: The Algerian defensive policy: legal and structural measures

Algeria is by far a promising growing country with considerable natural resources, and a strategic geographic location with convenient climate and stable political situation.

Those assets might be interesting for foreign investment or even tourism, but unfortunately, it is also a strong magnet for hostile cyber actions and attacks performed in reason of economic rivalry or as response to the Algerian honourable positions on just causes.

Accordingly, high authorities have launched serious awareness measures in order to contain the digital structures and networks' vulnerability to cyber threats; by issuing a brand new legal framework **(A)** and creating the necessary institutional structure **(B)**.

A) The legal framework

The Algerian constitution set an important principle stating that no felony or crime is recognized or punished without a legal text defining it.¹⁸

This principal comes along with the **article 54** recognizing the free-speech right and the liberty of information and ideas' dissemination but within the law's framework, to guaranty the respect of religious, moral and cultural values of the Algerian nation.

The constitution also reminds every citizen of their duty to undertake faithfully their obligations vis-à-vis national community and to safeguard national independence and sovereignty and the integrity of the whole national territory. It is everyone's duty to ditch any offending act that could be qualified as treason or even espionage, punished to the fullest extent of the law¹⁹.

Then, a legislative dynamic was initiated to ensure that internal law texts are lined up with international agreements signed by Algeria.

The Algerian legislator, for his part, promulgated the **law No. 04-15** on 10 November 2004 which defines, incriminates and set sanctions for felonies related to data integrity, confidentiality and security; by the amendment of the penal code at many articles (390 to 394 related to intellectual property and innovation protection).

Previously to this law, a fundamental amendment to penal code was promulgated back to 2001 (law 01-09)²⁰ in order to protect religious holy figures and heads of public institutions from adverse defamations and disrespectful allegations, spread especially on line.

Consequently, the legal arsenal incriminating cybercrimes was gradually built starting with a text of law No. 09-04 enacted on August 5th, 2009 in order to regulate **media, communication and messaging**, amended by **law No. 16-02**, defines cyber-crimes, and regulates the electronic communications surveillance.

Then, Law No. 10-05 of August 15, 2010 on competition was promulgated amending and supplementing ordinance No. 03-03 of 19 July 2003; to protect impartial commercial competition suffering of unfair e-commerce rivalry.

On 2016, Algeria officially initiated a national cyber security strategy²¹ adopting indeed a defensive- deterrent posture according to the fundamentals of its military doctrine, privileging the principle of non-interventionism but with permanent preparedness and vigilance²².

This strategy based on the anticipation of cyber-danger and threats and the foresight effort is directed to educate especially young generations to increase their awareness about that eminent danger.

Then, the **law No.18-05** for e-commerce enacted on 10 May 2018 represented Algeria opening to electronic trade and different transactions via internet and using e-payment legal channels. However, this law underlined the necessity of securing personal and payment data at rest and in transfer, in order to counteract money laundering.

However, the most waited for text was the **law No.18-07** enacted on 10 June 2018 on protection of natural persons in personal data processing.

This law provided the definition of **personal data** as any information associated to an identified or identifiable person, and **sensitive personal data** as well emphasizing specific information about a person's race, ethnic origin, religion or opinion.

Subsequently, the **law No.20-05** enacted on 20 January 2020 was promulgated on 28 April 2020 for the prevention and fight against discrimination and hate speech.

Indeed, digital world became a den of the spreading of that kind of phenomenon, which is particularly dangerous to national unity, tolerance and peaceful coexistence.

Moreover, an important **ordinance No. 21-09** reinforced the whole legislative arsenal, enacted on 8 June 2021 related to the protection of administrative data and documents.

This law set a protection system of administrative information and classified documents in reason of their value and sensitivity, in order to secure their access and avoid any leakage.

In addition, this law obliges public authorities to efficiently secure their documents and limit the access to them through a clear authorization system.

Nevertheless, the legislator recommends that any measure should be carefully initiated without infringing citizen's right to information.

These new legal provisions criminalize confidentiality assaults and provide for penal sanctions to deter strongly criminals²³.

Thus, the legal arsenal surrounding cyber-security issues seems rich in texts but in fact, it needs a permanent update because of the fast metamorphose of the digital sphere, and hackers constantly find out new means and techniques to overcome prevention measures.

It is a common feature characterizing all issues raised in modern era and challenging the legislator's reflex to keep up and learn from the best practices all over the world, to identify a phenomenon and regulate peoples' behaviour toward it.

In fact, a strong proactive institutional structure is necessary to accomplish that mission and recommend the necessary measures.

B) The institutional structure

Algerian high authorities decided to allocate the necessary financial resources to its digital infrastructures and increase their capacity to serve the population and institutions connected to internet and insure their safety²⁴.

The large capacity and diversity of digital services offered, create inevitably national networks and databases' vulnerabilities, and arouse the interest of hackers and cyber-criminals.

That is why Algeria also invested in creating institutions charged with cyber-security issues:

- **The Central Department for Combating Information Crime (SCLC)**, linked to the national security directorate. This entity is managed by highly skilled engineers recognized at national and international levels.

- **The Center for Prevention of Computer and Information Crime (CPLCIS)**, depending of national Gendarmerie and placed under the direct responsibility of the General Attorney

- **The National Institute of criminal Evidence and Criminology (INCC)**, depending as well of the National Gendarmerie. The institute is specialized in crime scenes investigation but those last years; cybercrimes took over this organism's usual intervention.

- **The postal and electronic communications regulation authority**: created since 2000 by the law 2000-03 repealed and replaced by the **law No. 18-04**. The legislator changed its name from wire and wireless communications and reinforced its autonomy for the decision making process.²⁵

- **The national committee for preventing and fighting offenses related to information and communication technology**, created by **law 09-04** enacted on 5 august, 2009 amended by law 16-02 regrouping national sectors concerned by cyber-threats' surveillance and prevention.

- **The national information security systems Council**, established by law 20-05 enacted on 20 January 2020, and it is affiliated to the ministry of national defence and charged with the development of a national strategy for security of information systems

- **The national authority for the protection of personal data**: created by the law 18-07 and established since august 2023. This independent authority is in charge of ensuring the accordance of personal data processing with law and the appropriate use of information and communication technologies respectfully to individual's rights and confidentiality²⁶.

- **The national information security repository (NISR- 2020)** establishing a common governance to ensure information security within organizations and companies. The NISR recommend the minimum requirements needed to face cyber-threats.

- **Higher national school of cyber-security**: created by the **presidential decree No. 24-181** and affiliated to technological pole, to ensure high studies for engineers and scientific research related to cyber-security.

An important contribution is expected from this institution to the national research effort for digital systems security as innovative solutions provider.

To conclude this segment, we can notice the rich institutional architecture devoted to cyber security issues, but a harmonization of tasks is necessary to facilitate each one's intervention and stay ahead of cyber-criminals.

Conclusion

The international increasing awareness of cyber-crimes over digital sovereignty needs a responsible international community sharing the same values about national security.

Sovereignty's erosion and decay phenomenon, which has been observed for years, changed its shape in reason of globalization's new issues.

The world was overwhelmed by the technology advance and the huge opportunities offered by efficient networks and internet increasing democratization.

However, expansionist intentions took over some powerful countries common sense, and they diverted the use of digital tools transforming them into lethal weapons.

At that point, rational nation-states privileged the defensive and preventive approach, under cover of international law.

This honourable journey needed a homecoming to firm principles prevailing the absolute respect of State sovereignty over its whole territory even digital space and frontiers.

Algeria, as unwavering peacemaker country preferred the defensive doctrine associated to digital empowerment, by strengthening its legal arsenal and institutional actors.

Unfortunately, despite the Algerian governments' efforts to enhance cyber- culture and to reinforce the legal and institutional cyber-security framework, it still ranked and classified as high-risk country toward cyber-criminality because of the vulnerability to malware infections.

The **Global Organized Crime Index** regrettably reported several breaches and insufficiencies concerning mainly the fragmented legislative arsenal and the limited competence and expertise of cyber-security institutions²⁷.

cyber-security engineers and specialists deplore a lack of recognition or career growth opportunities, and when they are approached and appealed by multinational foreign firms with huge contracts, they leave for a better career offer.

Recommendations:

The legislative "machine" must perform permanent legal texts' monitoring to keep up with new defence techniques and cyber threats.

The idiom says that the best way of defence is attack, so the Algerian authorities should:

- Initiate a "bug bounty" program, which is an award system for reporting cyber-security breaches accidentally found by researchers and developers, to encourage them and permit them to trace the institution in charge of that kind of information's processing;
- Create an internet platform regrouping all the actors and recognized organs;
- Privilege international cooperation and data exchange to reinforce the universal legitimate respond;
- Fund scientific research associating security engineers to constitutional and international law specialists in order to increase the scientific community's interest for debating the sovereignty issues regarding technological challenges.

- ¹ Fatiha BENABBOU –KIRANE, **Introduction au Droit Constitutionnel**, OPU, Alger, 2016, p 19
- ² David JORDAN, **the revolutionary career of Maximilien Robespierre**, University of Chicago Press, 1989
- ³ Martin LOUGHLIN, **the erosion of sovereignty**, Netherlands journal of legal philosophy, the London School of economics and political Science, 2016, p 64
- ⁴ Patrick GLENN, **The cosmopolitan State**, Oxford University Press, London, 2013, p 243
- ⁵ Martin LOUGHLIN, p 57
- ⁶ Martin LOUGHLIN, p 58
- ⁷ Article 14
- ⁸ Article 15
- ⁹ Pr. Fatiha BENABBOU –KIRANE, Op.cit, p 78
- ¹⁰ Matthias BRAUN and Patrick HUMMEL, **Is digital sovereignty normatively desirable ?**, information, communication & society journal, Rutledge Taylor & Francis group, 2024, p 6
- ¹¹ www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches
- ¹² www.fortinet.com/uk/ressources/cyberglossary
- ¹³ Leila BOUCHTAOUI, **from prohibition to empowerment: the challenge of connected generation**, Antidox, January 10th, 2025
- ¹⁴ Rihab YOUSFI, **cyber security challenges and international cooperation « balancing personal Data protection and information sharing»**, Journal of law and human sciences, volume 17, No. 3, 2024, p 39
- ¹⁵ Martin LOUGHLIN, Op.cit, p 57
- ¹⁶ Duncan HOLLIS, **a brief primer on international law and cyberspace**, June 14, 2021 (<https://carnegieendowment.org/posts/2021>)
- ¹⁷ Meriem LOUKAL, **study on the African union convention on cyber-security and protection of personnal data of 2014**, legal and economic studies journal, volume 04, No. 03, 2021, p 657
- ¹⁸ article 34 and 139 of the constitution
- ¹⁹ art 79 and 80 of the constitution
- ²⁰ Law No. 01-09 promulgated on June 26th , 2001
- ²¹ Référentiel National de Sécurité de l'Information, 2016 (www.mpt.gov.dz/wp-content/uploads/2023/12)

²² Lotfi SOUR, **Understanding Algeria's updated Military Doctrine in regional unrest context**, world politics journal, volume 6, No 1, 2022, p 1373

²³ Yahya TOUMI, **legal protection of administrative information and documents in the light of Law No. 21-09, an analytical study**, legal and political Algerian journal, Volume 7, No. 02, 2022, p 258

²⁴ The country's internet penetration jumped from barely 4% in 2007 to over 42 % in 2021.

²⁵ Dr. Aicha FAREH, **legal status of the postal and electronic communications regulation authority under the law 18-04**, legal and political sciences journal, volume 10, No. 02, university of El Oued, September 2019, p 392

²⁶ **Data protection laws of the world-Algeria** (www.dlapiper.com)

²⁷ Abdeljalil FORTAS, 30 July 2024 (<http://state-of-algeria.dev>)

Bibliography:

A- Books:

Fatiha BENABBOU –KIRANE, **Introduction au Droit Constitutionnel**, OPU, Alger, 2016

B- Scientific journal articles:

- Aicha FAREH, **legal status of the postal and electronic communications regulation authority under the law 18-04**, legal and political sciences journal, volume 10, No. 02, university of El Oued, September 2019

- David JORDAN, **the revolutionary career of Maximilien Robespierre**, University of Chicago Press, 1989

- Martin LOUGHLIN, **the erosion of sovereignty**, Netherlands journal of legal philosophy, the London School of economics and political Science, 2016

- Matthias BRAUN and Patrick HUMMEL, **Is digital sovereignty normatively desirable?**, information, communication & society journal, Rutledge Taylor & Francis group, 2024

- Meriem LOUKAL, **study on the African union convention on cyber-security and protection of personal data of 2014**, Legal and economic studies journal, volume 04, No. 03, 2021

- Patrick GLENN, **The cosmopolitan State**, Oxford University Press, London, 2013

- Rihab YOUSFI, **cyber security challenges and international cooperation « balancing personal Data protection and information sharing»**, Journal of law and human sciences, volume 17, No. 3, 2024

- Lotfi SOUR, **Understanding Algeria's updated Military Doctrine in regional unrest context**, world politics journal, volume 6, No 1, 2022

- Yahya TOUMI, **legal protection of administrative information and documents in the light of Law No. 21-09, an analytical study**, legal and political Algerian journal, Volume 7, No. 02, 2022

C – Specialized press articles

- Leila BOUCHTAOUI, **from prohibition to empowerment: the challenge of connected generation**, Antidox, January 10th, 2025

- Duncan HOLLIS, **a brief primer on international law and cyberspace**, June 14, 2021 (<https://carnegieendowment.org/posts/2021>)

D – Web sites

- **Référentiel National de Sécurité de l'Information**, 2016 (www.mpt.gov.dz/wp-content/uploads/2023/12)
- **Data protection laws of the world-Algeria** (www.dlapiper.com)
- www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches
- www.fortinet.com/uk/ressources/cyberglossary