Laurent Chrzanovski
Professor University of Sibiu (Romania), Visiting Professor Universities of Geneva (Switzerland), Lyon (France) and Varsovia (Poland)

Stephane Mortier
Associated lecturer Université Gustave Eiffel (DICEN Laboratory - Information and communication devices in the digital Era) and Research Centre of French National Gendarmerie (CREOGN)

THE DICHOTOMY OF USES OF ARTIFICIAL INTELLIGENCE IN NATIONAL SECURITY

THE DICHOTOMY OF USES OF ARTIFICIAL INTELLIGENCE IN NATIONAL SECURITY

Abstract: Artificial intelligence is probably the most important vector of security and law enforcement transformation. The need of security is a response to the defense of fundamental interests of states. How to protect these interest with artificial intelligence tools and technologies from foreign states? Beyond the major state powers, it is necessary to address the economic environment of artificial intelligence. The main players in the development of artificial intelligence in the world are the largest technology companies: GAFAM (Google, Apple, Facebook-Meta, Amazon, Microsoft) and BATHX (Baidu, Alibaba, Tencent, Huawei, Xiaomi). The reality is that their capacity to influence extends beyond the borders of the United States or China and their power is not limited to companies, but extends to States, NGOs, international and regional organizations. This hegemony is a reality also in Europe.

Most of the EU countries have the graeco-roman "modus vivendi" that requires new laws before the implementation of any single novelty in a court. In a world where new technologies, apps, softwares, appear on a daily base, we have no more time for that.

Resumen: La inteligencia artificial es probablemente el vector más importante de la transformación de la seguridad y la aplicación de la ley. La necesidad de seguridad responde a la defensa de los intereses fundamentales de los Estados. Cómo proteger estos intereses con herramientas y tecnologías de inteligencia artificial frente a Estados extranjeros? Más allá de las grandes potencias estatales, es necesario abordar el entorno económico de la inteligencia artificial. Los principales actores en el desarrollo de la inteligencia artificial en el mundo son las mayores empresas tecnológicas : GAFAM (Google, Apple, Facebook-Meta, Amazon, Microsoft) y BATHX (Baidu, Alibaba, Tencent, Huawei, Xiaomi). La realidad es que su capacidad de influencia va más allá de las fronteras de Estados Unidos o China y su poder no se limita a las empresas, sino que se extiende a los Estados, las ONG y las organizaciones internacionales y regionales. Esta hegemonía es una realidad también en Europa. La mayoría de los países de la UE tienen el "modus vivendi" graeco-romano que exige nuevas leyes antes de la aplicación de cualquier novedad en un tribunal. En un mundo en el que cada día aparecen nuevas tecnologías, aplicaciones y programas informáticos, ya no tenemos tiempo para eso.

Keywords: Artificial intelligence, security, fundamental interests, dependency

Palabras clave: inteligencia artificial, seguridad, intereses fundamentales, dependencia

1.- INTRODUCTION

In 1996, in an article entitled "The World Wide Web as Super-Brain: from Metaphor to Model", Francis Heylighen and Johan Bollen of the Vrij Universiteit Brussel (VUB) put forward some interesting proposals concerning the development of the "super-brain" and what enables it to learn, without omitting to point out that it is not the brain itself that thinks, but the users of the web. Indeed, the power of this "super-brain" lies in the tenuous link with its users, a self-referential link. Algorithms have also developed, which (by analogy with the human brain) strengthen the links and weakens those that are less frequently used. Using the principle of transitivity, the construction of new links can be automated. But none of this means that this "super-brain" can actually think independently of the users that make it up (Mortier, 2019). Today, the conditions are ripe for a widespread evolution of Artificial intelligence technology techniques: availability and diversity of data, development of offers and performance of IT devices and equipments (Marellin, 2021).

We will use here the concept of artificial intelligence and artificial intelligence system as defined by the European Parliament1 : "Artificial intelligence (AI) refers to the ability of a machine to reproduce human-related behaviours, such as reasoning, planning and creativity. AI enables technical systems to perceive their environment, manage these perceptions, solve problems and take actions to achieve a specific goal. The computer receives data (already prepared or collected via its sensors – a camera, for example), analyses it and reacts. AI-enabled systems are able to adapt their behaviour (more or less) by analysing the effects of their previous actions, working autonomously".

The Artificial Intelligence (AI) has giant possibilities to optimize the fight against crime and strengthen national security. In the conditions of unimaginable accumulation of information and the need for rapid decision-making, only the use of AI can lead to success. Intelligence, counterintelligence, forensic science, counteracting organized crime, rapid processing of available information, drafting of varied decisions, creating plans and multivariate scenarios, performing various analyzes is a time-consuming process. Only its use can significantly shorten this time and thus dramatically increase the possibilities for detection, prevention and curbing crimes (Radulov, 2019). In brief, Artificial Intelligence (AI) and Machine Learning (ML) can be a great cyber defense strategy, it can also be a double edged sword (Meghani, Essomba, Chrzanovski, 2023).

Artificial intelligence is and will increasingly be indispensable for national security. It is inconceivable to exclude such technology from security strategies. More and more, the regalian services are using artificial intelligence tools, both for judicial investigations and for intelligence or administrative police. For example, the French Gendarmerie Nationale has developed an "artificial intelligence platform" which was awarded the Europol Excellence in Innovation Award in 2022. This AI platform provides its user with a suite of advanced criminal analysis tools, specifically developed to meet the needs of investigators when processing criminal information. It includes a text comparison tool, image-based object detection (weapons and drugs), speech-to-text transcription, entity extraction, and machine translation tools in over 100 languages2. At European level, The

[1] https://www.europarl.europa.eu/news/fr/headlines/society/20200827STO85804/intelligence-artificielle-definition-et-utilisation

[2] https://www.gendarmerie.interieur.gouv.fr/gendinfo/actualites/2022/europol-la-gendarmerie-recompensee-pour-sa-plateforme-d-outils-d-intelligence-artificielle-i.a.

EU-funded AIDA project (2020-2023) focuses on cybercrime and terrorism by addressing specific problems related to law enforcement agencies (LEAs), using state-of-the-art methods based on machine learning and artificial intelligence. The project will provide a descriptive and predictive data analysis platform and associated tools to prevent, identify, analyse and combat cybercrime and terrorist activities. The platform is based on core technology applied to Big Data analytics, with extensive AI and deep learning techniques customised with additional crime-specific capabilities and tools3. This project, led by "Engeneering/Ingegneria Informatica SPA", the Digital Transformation Company leader in Italia, is composed of a consortium of 21 partners, including Europol and seven law enforcement agencies (LEA) from seven EU member states : Guardia Civil (Spain), Hellenic Police (Greece), Police Service of Nothern Ireland (United Kingdom), Inspectoratul General al Politiei Romane (Romania), Policia Judiciaria (Portugal), Nationale Politie – Landelijke Eenheid (Netherlands), Estonian Police and Border Guard Board (Estonia). The resultswill be published in the coming months on the project website4.

While AI is a major technology destined to spread across all sectors of activity, its speed of deployment also creates an increased risk of failure and represents a safety and resilience issue at national and international levels (Institut Montaigne, 2023). With increased resources – including private resources – the US and China have substantial lead in the economic and technological development of AI. Europe has thus accumulated a delay that is difficult to make up. In a 2022 report, the Skema Publika thinh tank, over the last 30 years, more than 860,000 patents related to artificial intelligence have been filed. The origin of these patents is as follows[5] : United States (30%), China (26%), Japan (12%), South Korea (6%), Germany (5%), United Kingdom (2.5%), France (2.4%) and Canada (1.9%). The US and Asian powers thus account for almost three quarters of the AI innovation market. Yet the European Union is preparing to impose safety and trust requirements on AI systems through specific regulations (AI Act) and has a lot of high quality researchers in mathematics and artificial intelligence.

The risk is not in the use of artificial intelligence but in the algorithms or tools based on it that enable its use. Most of the algorithms and tools are developed outside the European Union and place the Member States in a certain form of dependence on foreign powers. This of course generates risks for national security and the protection of the fundamental interests of European states.

After reviewing the context in which artificial intelligence is evolving and becoming inescapable, we will address, through concrete cases, the risks to which European countries are currently exposed.

[3] https://cordis.europa.eu/project/id/883596/fr
[4] https://www.project-aida.eu/index.php
[5] https://www.cio-online.com/actualites/lire-l-europe-a-la-traine-pour-les-brevets-autour-de-l-ia-14132.html

2.- NATIONAL SECURITY ENVIRONMENT

2.1.- A non-territorialized cyberspace: Dystopia or Utopia?

It is commonly accepted that the notion of territory comes from the Latin territorium for territory as an area of land occupied by a human group. This is indeed a physical dimension (area of land) with a human presence, a human occupation. However, there is another, less well-known meaning, derived from *terrere*, meaning "to frighten", "to terrorise". Hugo Grotius makes a more than pertinent analysis in *De jure belli ac pacis* at the beginning of the 17th century:

"*This is why Siculus Flaccus derives the word territory [...] from a Latin verb "terrendis hostibus", which means to frighten, because, he says, the one who is master of it frightens the enemies: an etymology that seems as well founded as the one that others give. Varron derives the word territory from the verb "terrere", to trample under foot, Frontinus derives it from the word "earth", the jurisconsult Pomponius, from the same word, as Siculus Flaccus, but for another reason, he says that the magistrates have the right to frighten within the territory".*

The physical dimension is less pronounced in this sense. Indeed, "to frighten" is behaviours, mean to control other behaviours and consequently the behaviours of humans in a given context, in a given space controlled by an authority. Although this space is a physical territory in Grotius's words, "frightening" or "frightening" could be relative to a virtual, abstract, non-territorialised space in the primary sense of the word.

This is where the term cyberspace comes in, and its origin is particularly rooted in this scary side. Indeed, it appears in 1984 in a science fiction novel (*Neuromancer* by William Gibson) where it is defined as "*A consensual hallucination experienced daily in all legality by tens of millions of operators, in all countries, by kids who are taught the concepts of mathematics... A graphic representation of data extracted from the memories of all the computers in the human system. An unthinkable complexity. Lines of light arranged in the non-space of the mind, clusters and constellations of data. Like city lights, in the distance...*". This is a totally new world, totally extra-territorialized, "scary". This work of science fiction belongs to the literary genre called "cyber-punk". This literary genre describes a violent, dark, near-apocalyptic world where computer technology and artificial intelligence are at the heart of the functioning of society. In this sense, this literary genre is close to dystopia, which is nothing other than an impediment to achieving happiness, a chaotic world.

On the other hand, another vision of cyberspace, a rather utopian one, is defended by other circles. The Global Information Infrastructure (GII) project promoted by Al Gore in the United States in 1993-1994 confirmed this utopian trend. In 1994, he declared before the International Telecommunications Union:

"The Global Information Infrastructure (GII) will not only be a metaphor for a functioning democracy; it will actually encourage the functioning of democracy by enhancing citizen participation in decision making. It will promote the ability of nations to cooperate with each other. I see it as a new Athenian age of democracy forged in the forums that the GII will create".

But the high point came two years later, in 1996, with John Barlow's "*Declaration of Independence for Cyberspace*6". It is certainly the strongest element of this representation. It is, in more than one way, evocative. Indeed, it clearly resembles a new ideology based on a virtual, infinite and impalpable space and, above all, in opposition to the physical world shared between nation-states and where these states are neither welcome nor able to control cyberspace:

"In China, Germany, France, Singapore, Italy and the United States, you try to contain the virus of freedom by erecting guard posts at the borders of Cyberspace. These may contain the contagion for a while, but they won't work in a world that will soon be covered in digital media".

Here is something to "scare" the nation states! neither utopia nor dystopia but a fourth space freed from its physical dimension. Territories and borders are indeed the foundations of their existence and survival... However, in the physical world, these two notions are tending to erode somewhat. By way of illustration, let us cite two examples: the "Shengen area" and tax optimisation. The Shengen area, apart from the picturesque charm of the Luxembourg village, is an area of free movement of goods, capital, services, and people that includes the 27 states[7] that have signed this agreement. The principle of the free movement of persons[8] means that any individual (EU or non-EU national[9]), once he or she has entered the territory of one of the member states, can cross the borders of the other countries without being subject to systematic controls. Air flights between cities in the Schengen area are considered as domestic flights without control of biometric passports (personal data that may be used in an IA system). Finally, are not tax optimisation techniques a means of circumventing certain borders and therefore the authority that is exercised within them, i.e. on a given territory? It consists of onshore or offshore techniques and methods that can be used to reduce the tax burden on both individuals and companies. This is done in a completely legal way (unlike evasion which is illegal), the taxpayer having the right to seek, and use, the least taxed route. In short, through these two examples, it is clear that the notions of border and territory are being eroded little by little, through the surrender of sovereignty in one case, through legal circumvention in the other. To this we could add civil society movements such as "No Border[10]", an international network that fights for a world... without borders.

3.- ARTIFICIAL INTELLIGENCE AND CYBERSECURITY: WHAT SECURITY IN CYBERSPACE?

Whether the vision of cyberspace is dystopian or utopian, it raises the question of the alteration or even disappearance of borders. This does not, however, dispense with the physical existence that characterises cyberspace. The official definition of the French State services such as the National Agency for the Security of Information Systems

[6] American libertarian poet and activist who died in 2018, co-founder of the Electronic Frontier Foundation (an NGO dedicated to defending free speech on the internet).

[7] Except Bulgaria, Cyprus, Ireland and Romania, all EU states are part of the Schengen area. Switzerland, Liechtenstein, Iceland and Norway are also members. The status of Gibraltar is still under negotiation as part of the Brexit agreement.

[8] Article 3 of the EU Treaty

[9] The Entry/Exit System (EES) is implemented by the European Union and will be operational in May 2023. The system aims to register the entry and exit of non-EU citizens crossing an external border of the Schengen area. It stores identity and travel document data as well as biometric data.

[10] See the network's website http://noborder.org/

(ANSSI) or the Ministry of Europe and Foreign Affairs (MEAE) attests to this: "A space of communication constituted by the worldwide interconnection of automated digital data processing equipment and by the objects connected to it and the data processed therein". The communication space is virtual, the equipment and infrastructure are essentially material (the storage can be immaterial – cloud) and the data processed is... immaterial. If the cyberspace is a fourth space without physical dimension, how to express sovereignty on data, except on physical storage devices? More especially in the case of AI, who owns the algorithms and training data?

The concept of digital sovereignty can be understood in a different sense and refer to the ability of a given entity (a nation, a company, an individual) to master digital attributes (data, information, knowledge, algorithms) on objects that it claims to observe or even control. The term "control" does not necessarily mean that the entity holds (in the sense of full ownership) the objects in question, and *a fortiori* the digital attributes, in this case the data, of these objects (Ganascie, Germain, Kirchner, 2018)[11]. This is how digital sovereignty is conceived in France and more widely in Europe. It is indeed the (immaterial) data that represent the challenge of this sovereignty. In this respect and with this in mind, the European Union has a legislative arsenal in this area.

On 23 June 2022, the new European Data Governance Act (DGA) officially entered into force. It will take effect in September 2023.

This text is part of the "European Data Strategy*12"*, itself a sub-branch of the strategy "Shaping Europe's Digital Future*13"*, unveiled in February 2020 by the European Commission, of which one of the six priorities for the period 2019-2024 is to "adapt Europe to the digital age*14"*. To this end, the European Union has undertaken, in particular, to equip itself with new legal instruments in the field of the platform economy (Digital Markets Act15 and Digital Services Act16), and artificial intelligence (Artificial Intelligence Act17), and, of course, in that which concerns the raw material of the digital economy: data.

The most important and relevant legislative initiative is the draft Artificial Intelligence Act, the first ever European legal framework dedicated to AI systems. The Commission has chosen not to regulate AI itself as a technology, but to focus on AI systems, understood as software capable of generating outputs such as content, predictions, recommendations or decisions (Article 3 of the draft AI Regulation), and to use a multi-layered risk-based approach. Some uses of AI entail an unacceptable risk and are prohibited; others create a high risk and are allowed if their providers meet certain

[11] Available on : http://cerna-ethics-allistene.org/digitalAssets/55/55160_AvisSouverainete-CERNA-2018-05-27.pdf

[12] European Commission, « A European Data Strategy », Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 19 February 2020.

[13] European Commission, « Shaping Europe's Digital Future », Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 19 February 2020.

[14] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_fr.

[15] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52020PC0842

[16] https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 and https://artificialintelligenceact.eu/the-act/

requirements and carry out a compliance assessment. Uses that are considered low or minimal risk are simply allowed. Uses of AI that undermine fundamental values are considered unacceptable risks. But the text but provides some exceptions like (the search for potential victims of crime, including missing children; certain threats to the life or physical safety of individuals, including terrorist attacks; and the detection, location, identification or prosecution of perpetrators or suspects of criminal offences of at least three years – art. 5 and whereas 19[18]). These include systems that deploy subliminal techniques, exploit vulnerabilities to alter human behaviour, or are used for algorithmic social rating. Finally, the use of "real-time" remote biometric identification of people in public spaces is considered particularly intrusive and is in principle prohibited (Ponce del Castillo, 2021) [19].

It is therefore through security (cybersecurity), of immaterial data in particular, that the real world is trying to "master" cyberspace. It is an attempt to territorialise the dematerialised without possessing the material element: a decorrelation between the territory and the space of sovereignty (non-territorialised) (Mortier, 2020).

Cybersecurity therefore allows the expression of "digital" sovereignty. It is defined by the ANSSI20 as the state sought for an information system enabling it to resist events originating in cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and the related services that these systems offer or make accessible. Cybersecurity involves the use of information systems security techniques and is based on the fight against cybercrime and the establishment of a cyber defence. This definition includes purely sovereign elements such as the fight against crime and defence, but relates to the data that is coveted in cyberspace.

As for artificial intelligence, what place does it occupy in the field of cyberspace and more particularly in the expression of sovereignty within it? AI is a disruptive technology that is gradually being implemented, while cybersecurity is about the security of digital infrastructures and the digital safety of users. However, some AI processes can help to create safer cyber spaces. An artificial intelligence system is an automated system that, for a given set of human-defined objectives, is able to make predictions, recommendations, or decisions affecting real or virtual environments. A such system functions through algorithms that attempt to reproduce human intelligence on a probabilistic and deterministic basis through the processing of large volumes of data. These algorithms, these computer programs, constitute the basis of artificial intelligence and are the result of a process of creation by humans, hence the term artificial. It is not a natural process but an artificial construction. Machine learning, a field of artificial intelligence, aims to enable a machine, through the use of learning algorithms, to determine the best possible result or, if necessary, to detect malicious behaviour in cyber security for example. To work, this "method" needs access to data. This brings us back to the immaterial and virtual characteristics that allow the expression of digital sovereignty over a non-territorialised space (cyberspace in which the data is located) (Mortier, 2020).

[18] https://artificialintelligenceact.eu/the-act/

[19] Available on https://www.etui.org/sites/default/files/2022-03/04_La%20strat%C3%A9gie%20num%C3%A9rique%20de%20l%E2%80%99Europe_2022.pdf

[20] Agence Nationale de la Sécurité des Systèmes d'Information / National Agency for the Security of Information Systems https://www.ssi.gouv.fr/

Today, our understanding of what is AI varies with the passing of each milestone in this field. Adaptability, flexibility, predictability and proactivity in terms of minimum time resources, the speed of decision-making and scenarios realizing them should be the priorities of the AI used in the security sphere (Radulov, 2019).

In this sense, artificial intelligence, made up of algorithms and computer programs, would be only one of the physical aspects of the networks mentioned above in the definition of cyberspace proposed by the French authorities: "... worldwide interconnection of automated digital data processing equipment...". Artificial intelligence could then return to a more conventional understanding of sovereignty since the algorithms that give it life would have a nationality by virtue of their creation by a human being who, for the time being, holds a nationality relative to a classic expression of sovereignty.

These few reflections on territory, borders and sovereignty are in no way intended to be exhaustive or peremptory, but rather to raise awareness of the fact that human nature always tries to bring together what is known with what can sometimes be beyond it. A natural reinterpretation of the immaterial in order to keep one's own reference points. The shock of digital technology, the shock of cyberspace, which has arrived like a wave in a few decades (close to zero on the scale of humanity), requires man to rethink his condition in a world that is both new and still marked by an inescapable existing. From a "black transcendence" (Hottois, 1984) to a "re-enchantment of the world", everything is possible and the tone seems to be set by... data, artificial intelligence, the link between the real world and cyberspace, between utopia and dystopia, both of which are equally "frightening", but also the object of law, security and the foundation of an intelligence created by man, artificial.

4.- ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY: A DEAD END?

National security, for a company, a citizen or a strategic and sovereign State, is defined as the fact of being able to have full control over its data. And this also implies knowing how to defend oneself legally, economically and technologically from other supplier states – or foreign companies – for the storage, capture and exploitation of data (Decloquement, Luttrin, 2023).

The French Penal Code defines the fundamental interests of the nation, the objects of national security, as follows (art 410-1) :

"its independence, (...) the integrity of its territory, (...) its security, (...) the republican form of its institutions, [the] means of its defence and (...) its diplomacy, (...) the safeguarding of its population in France and abroad, (...) the equilibrium of its natural environment and its surroundings and [the] essential elements of its scientific and economic potential and of its cultural heritage."

A state therefore has an obligation to safeguard its sovereignty in this way. In order to do this and to deal with threats, it must have the necessary resources, including technology. Artificial intelligence is now a component of this because of the developments it suggests. The defence of fundamental interests is no longer limited to the physical plane, but also encompasses the virtual domain.

The major national security risk in the use of artificial intelligence is the dependence on foreign technologies. There is indeed a real technological competition between the United States and China. The investments of these two powers in European companies are fully in line with this competition. It is particularly difficult for European states to coordinate in order to combat this type of economic predation, despite the European foreign investment screening mechanism. European states are therefore becoming increasingly technology importing countries. This can take the form of access to biased information or strategic operations by foreign powers: the use of algorithms developed and controlled by them creates not only dependence but also risk. Moreover, artificial intelligence controlled by someone else opens the door to the risk of cyber-attacks, the manipulation of content and even the misappropriation of strategic informations. Even further, a foreign power could control the social control of our populations and thus set up disinformation actions to destabilise the social order.

In terms of intelligence, the United States is deploying considerable resources to master artificial intelligence. The Central Intelligence Agency (CIA) alone has around 140 projects in development that leverage AI in some capacity to accomplish tasks such as image recognition and predictive analytics. The Intelligence Advanced Research Projects Activity (IARPA), whose mission is to devise and lead high-risk, high-impact research leading to innovative technologies with significant future benefits for intelligence, is sponsoring several AI research projects intended to produce other analytic tools within the next four to five years. Some examples include developing algorithms for multilingual speech recognition and translation in noisy environments, geo-locating images without the associated metadata, fusing 2-D images to create 3-D models, and building tools to infer a building's function based on pattern-of-life analysis (Congressional Research Service, 2020). Such means are not available to European states without real multilateral cooperation. The AIDA project, mentioned in the introduction, is the beginning of a European response but probably lacks dimension.

Beyond the major state powers, it is necessary to address the economic environment of artificial intelligence. The main players in the development of artificial intelligence in the world are the largest technology companies. GAFAM (Google, Apple, Facebook-Meta, Amazon, Microsoft) are economic monsters, of unprecedented size, sometimes in a position of near-monopoly, which gives them enormous power (Cazals, Cazals, 2020). The reality is that GAFAM's capacity to influence extends beyond the borders of the United States and their power is not limited to companies, but extends to States, NGOs and even international organisations (Nour, 2019). The hegemony of the GAFAMs in Europe is almost complete. In November 2021, at the peak of the COVID-19 pandemic, the GAFAMs reached record margins: 38% for Microsoft, 37% for Meta, almost 30% for Google and over 26% for Apple 7. In early December, the latter's market capitalisation reached the highest ever recorded for a US company at a staggering $2,650 billion, followed by Microsoft ($2,570 billion), Alphabet ($1,980 billion), Amazon ($1,850 billion) and Meta ($1,000 billion) (Smyrnaios, 2023). Although they are economic actors, they are and represent foreign forces whose modus operandi is as follows :

- Analyze targets (psychological weaknesses, economic and social weaknesses and social weaknesses, modes of operation, network, family and professional environment, identification of the needs of the territory) ;
- Use psychological vulnerabilities and respond to a specific need in the territory (short-term strategy) ;

- Penetrate the territories, impoverish them (in the medium and long term) to better absorb the State (Decloquement, Luttrin, 2023).

On the Chinese side, on its territory, Beijing obliges foreign companies, including American ones, to collaborate with a Chinese counterpart, to store their data, even the most sensitive ones, locally and to transmit their technological patents, at the risk of losing access to the market of the second world economy (Nour, 2019). This is one of the reasons for the huge developments in artificial intelligence in China. In the United States, much of the data is monopolised by private companies (Amazon, Facebook and Google), whereas in China the majority of companies are either public or linked to the government in some way. Therefore, the plethora of data, thousands of entrepreneurs and engineers, as well as the active support of political power, are ingredients that facilitate this Chinese rise. Currently, the BHATX (Baidu, Huawei, Alibaba, Tencent, Xiaomi) combined have more data than the US and Europe combined (Nour, 2019). Similarly, one of the key components of AI, namely maching learning, which relies, essentially, on abundant data, is being further developed in China through two global leaders in mobile payments, namely AliPay and Tencent. Indeed, as surprising as it may seem, Chinese people make 50 times more mobile purchases than Americans (Nour, 2019).

5.- ARTIFICIAL INTELLIGENCE AND LAW ENFORCEMENT IN EUROPE

The roots of the problem having been laid down, we would like to draw up a short list of the elements specific to the EU and to each of its member states, rendering simply impossible to achieve an efficient AI system at the service of law enforcement and justice at the entire European Union level.

5.1.- The lack of will and means in the short, medium and long term

Recently, the website of one of the leading AI organizations – the Centre for Governance of AI, in Oxford – published a white paper with an intriguing title (Ord, 2022) : *Lessons from the Development of the Atomic Bomb*. This very pertinent text indirectly compares the resources needed by any state entity wishing to possess the atomic bomb with those needed by the same entity to develop its own operational AI system.

The previous pages largely evoke the infinite powers of Big Tech – to which we will add the (illegal) capacity of global surveillance, recently strengthened by the StarLink satellite constellations and soon to those of Amazon, all topics explained in great detail in the reference work on this subject, Shoshana Zuboff's masterpiece (2019).

On this subject, for the development of an atomic bomb as well as for the development of a sovereign complete AI system, the four main conditions explained by Orb (2022) are:

- to possess the raw materials (= what Europe does not have in terms of hardware)
- to have an unwavering political will in the short, medium and long term (impossible in the current state of the EU and national prerogatives)
- to have for decades the human, technological and financial resources needed (Europe has never had a single program quantified in trillions of Euros, the sum necessary for an AI system, all that has been implemented so far, all fields considered, not exceeding a few billions), and, finally,

- to perform active espionage of those who already possess the bomb (in this case AI) as well as to keep the most total secrecy on the development of the weapon itself (of AI).

The EU spying the GAFAM/BHATX and keeping a total secrecy on the existence and activity of the mega-laboratory developing its own AI system – including satellites, terrestrial hardware including quantum computers and supercomputers, own-made individual recognition software and means of capillary surveillance throughout the EU? One does not need to become as cynic as Emil Cioran to realize that if the development of a European security is already impossible, its extension to a pan-EU AI system as well as continuous EU operations of espionage, counter-espionage and deception (preserving the secrecy of the project) left in the hands of Brussels is pure science fiction.

5.2.- The everlasting choice of inter-EU competition instead of federation...

In the field of a fully functional AI system for security, the EU needs reliable and quick communications as well as top-notch technologies and, last but not least, a unique competence centre receiving, analysing and dispatching the investigations, in real time, to each EU member.

The choices made since the beginning of the EU's "digital decade" are just comparable with a small cashbox with 27 holes giving each member State Euros for achieving the same goal as every other member.

Two examples are particularly relevant : the first is, due to the U.S. political pressures, most of the EU members still lack 5G (not to speak about the very-soon available 6G), a fundamental element for the good functionality of AI. This refusal to adopt the last wireless technology is costing the EU's economy billions each year.

What has been the EU decision? To create a fund of 2 billion Euros to be distributed to each member desiring to create an operative OpenRan technology which, at the end, in 2027, will compete with the technologies developed by other members. Useless here to mention that France, Spain and Germany already master this technology : a logical business mind would have simply made an EU OpenRan combining the best of each of the result obtained by these three States and proposing it to the EU Parliament for an immediate adoption (Lauhde, 2022).

The second element, even more pertinent, is the "European Cybersecurity Center" as it was labelled ten years ago, to be under the direction of a newly created position of EU Commissioner. Set to be located in the UK, everything had to be re-thought after the Brexit. Many hopes were still possible until 2020, as the former head of Security of the IAEA was appointed to design its functional architecture, while Bucharest won the competition to host the Center's headquarters.

The entry in function of President von der Leyen and the elimination of the old "Spitzkandidaten" way to choose the Commissioners, doubled by economical (hence political) consequences of the COVID and the energy crisis, the ever-growing disputes between several member States had a catastrophic impact on all the project designed for the purposes of the Cybersecurity Center and not only as it has been highlighted in

December 2022 by the veto of only 2 members prohibiting Romania and Bulgaria to join the Schengen area while the unanimity of the members was welcoming Croatia.

The new born security entity suffered in its very roots. Re-branded ECCC (European Cybersecurity Competence Centre and Network), it is still directed by a steering committee (and not a Commissioner), and its goals are mainly to distribute funds and share know-how for any demanding member State.

Hence it will never become the wished pro-active law enforcement / intellligence agency of the Union, following the steps of the Council of Europre's C-Proc (Cybercrime Programme Office), also based in Bucharest, reduced by the very same national sovereignty political egos to perform continuous capacity building mainly in third world countries and sometimes in one the EC members.

5.3.- The european digital id, a fundamental tool for a future AI, approved by the EU but...

In March 2023, an overwhelming majority of the EU Parliament voted for the implementation of an EU digital ID. This would be another essential tool for any AI system dedicated to law enforcement purposes.

Alas, although the legislative text includes all the guarantees ensuring that each EU citizen will have a permanent right of access and surveillance to the data contained in this “digital passport” (which should/could eventually include tax, health, legal and biometric documents etc.), there is a majority of political parties against the participation of their country to the digital ID, in most of the EU countries and above all in the whole Eastern EU (where the memory of the communist times State intrusion in personal lives is still very pregnant, even by the youngest generations).

The EU digital ID, whose implementation and contents is let to the latitude of each member State, is very likely to become a gigantic empty folder, at least for a short and middle term.

5.4.- The european "AI act", an inescapable obstacle for a performant law-enforcement AI...

The above-mentioned act, finalized in 2021 but still not voted by the EU parliament, is an over-ethical text, which will probably boost EU-made AI sales to customers desiring to protect their clients' privacy, mainly in countries, where the citizens are very suspicious towards the intelligence activities of their own government – like the USA or Canada after Snowden's revelations and the Patriot Act abuses for the USA, after the judicial abuses during the martial law period enforced by the Trudeau government during the truck-drivers strike (Siegmann, Anderljung, 2022)

Paradoxically, as we can see in the USA, where AI is already used for law enforcement and justice purposes, this European rule, if implemented, will simply forbid the use of AI by the same actors in the EU, as no complete investigation realized with the help of a complete AI toolkit can be performed without “collateral damage” (environmental interceptions, video/pictures examination etc. are all elements where other citizens appear, aliens to the mischiefs of the investigated possible criminal). Even if all these elements can and must be duly censored and erased before the trial, this very

topic will be politically widely used, with the help of the EU's "AI Act", to take radical positions against the use of AI by law enforcement bodies.

5.5.- The momentum for AI used by law enforcement is probably the worse in recent history ...

Another vital source to analyse the AI via the perception of the EU's population and companies are all the white papers published by the Barcelona-based IE University – Center for the Governance of Change (ie.edu) and in particular its yearly report "European Tech Insights". Its hugest version, published in 2 volumes in 2021, underling a sort of "schizophrenia" within the perception of each individual on what is really AI (Chrzanovki, 2021). As a matter of fact, on the one hand, a huge majority of Europeans would like EU and its member states to take legal measures to reduce the loss of jobs due to AI and ML (European Tech Insights, 2021), but on the other hand, the mistrust for the actual political class and governments is total: a majority of Europeans clearly want the social media to censor fake news and not State institutions (European Tech Insights, 2021). Worse, 51% of the Europeans would prefer AI to rule their country instead of human congressmen and government members (European Tech Insights, 2021).

The main problem, in the field of our topic, is that we are witnessing the worse level of trust towards politicians and hence governments in contemporary history. The dramatic aspect is that the direct consequence of this lack of trust, even in countries where the administration fulfils the expectations of the citizens, law enforcement bodies and, above all, intelligence services are believed to be as toxic as the politicians, meaning that any new dotation to those entities (AI would be the biggest) is de facto considered as an intrusion into the citizen's privacy.

6.- CONCLUSION: SOME LIGHT AT THE END OF THE TUNNEL

There is a growing interest in Europe for the concepts of "digital sovereignty" and "strategic autonomy in cyberspace". Although their meanings are different, they are closely linked and both refer to the will of European political and economic actors to maintain their autonomy in their strategic decision process. For the European states, it involves acquiring an autonomous capacity of appreciation, decision and action in order to exercise their sovereignty (Dannet, Desforges, 2020). This is the heart of the matter: how to defend one's national interests when one is in a situation of dependence? Although efforts are being made within the European Union, particularly in terms of regulation, much remains to be done in terms of the development of artificial intelligence systems.

As we are very far to see the beginning of a draft of an integrated pan-EU AI system benefitting exchanges and performances of the law enforcement bodies (see the list of EU countries opposition to such a system in Viscusi, G, Collins, A., Florin, M.-V. 2020), the only way to follow, in our opinion, is to hope that a few courageous governments and supreme courts allowing the beginning of the use of AI in their territory.

Of course, the first step is to forbid, the so-feared "predictive AI", banned even by the USA as it could lead to results such as the ones watched in Steven Spielberg's masterpiece "Minority Report" (2002). If such a step is achieved, and AI is progressively introduced and admitted by courts, then we already have a European "good practices guideline" : the volume produced by UNICRI with Europol (UNICRI, 2018).

But, above all, we have the pragmatic experience of the US courts. After some years of allowing the use of AI, a complete list of mistakes as well as good achievements has been compiled. As a result, the very White House endorsed a comprehensive framework, with clear instructions to be followed by any AI user (company or institution) (Office of Science and Technology Policy, 2022).

Yet most of the EU countries have the graeco-roman "modus vivendi" that requires new laws before the implementation of any single novelty in a court. In a world where new technologies, apps, softwares, appear on a daily base, we have no more time for that.

Experimental phases, with or without a decisive value for the courts, are needed, if the EU does not want to continue to be the victim of the immense power of the GAFAM/BATX which follow Eric Schmidt's (then Google's CEO) 2011 statement: "*High tech runs three-times faster than normal businesses. And the government runs three-times slower than normal businesses. So we have a nine-times gap... And so what you want to do is you want to make sure that the government does not get in the way and slow things down"*.

BIBLIOGRAPHY

- Cazals, F. ; Cazals, C. (2020), "GAFAM et BATX contre le reste du monde", *in* Cazals, F. ; Cazals, C., *Intelligence artificielle. L'intelligence amplifiée par la technologie*, De Boeck Supérieur.
- Chrzanovski, L. (2021) , "ML, AI, IoT: why it is important to take the time to reflect", *Cybersecurity Trends*, UK Edition, n°3/4.
- Congressional Research Service (2020), *Artificial intelligence and National Security*, November.
- Danet, D. ; Desforges, A. (2020), "Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques", *Hérodote*, vol. 177-178, no. 2-3.
- Decloquement F. ; Luttrin A. (2023), "La souveraineté numérique au fondement de notre performance nationale", in Celcle K2, *Les enjeux du big data*, Cercle K2.
- *European Tech Inside* (2021), Center for the Governance of Change- IE University, Vol.1.
- Ganascie, J.-G. ; Germain, E. ; Kirchner, C. (2018), "La souveraineté à l'ère du numérique. Rester maître de nos choix et de nos valeurs", *CERNA*, May.
- Hottois, G. (1984), *Le signe et la technique. La philosophie à l'épreuve de la technique*, Aubier Montaigne, Paris.
- Institut Montaigne (2023), *Investir l'IA sûre et digne de confiance : un impératif européen, une opportunité française*, Note d'action, Avril.
- Mika Lauhde, M. (2022), "Par quel moyens serons-nous espionnés ou, au contraire, plus protégés demain: anciennes et nouvelles normalités des télécoms...", *Cybersecurity Trends, Edition Spéciale Cyber-espionnage économique et technologique*, Juin.
- Marcellin, S. (2021), "L'intelligence artificielle centrée sur l'humain: droit ou éthique?, *Revue de la Gendarmerie Nationale*, n°268, January.
- Meghani, R. ; Essomba, M. ; Chrzanovski, L. (2023), "The stakes have never been higher…", *CyberSecurity Trends*, UK Edition, n°1.
- Mortier, S. (2019), "Réflexion sur l'Homme et le cyberespace : le paradoxe de l'oeuf et de la poule", *Revue de la Gendarmerie Nationale*, n°266, December.
- Mortier, S. (2020), "IA et cyber-sécurité, les instruments de conquête d'un espace non-territorialisé", *Droit et Patrimoine*, n°298, January.
- Nour, M. R. (2019), "Géopolitique de l'Intelligence Artificielle : Les enjeux de la rivalité sino-americaine", *Paix et Sécurité Internationales*, n°7.
- Office of Science and Technology Policy (2022), *The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People,* The White House , October.
- Ord, T. (2022), *Lessons from the Development of the Atomic Bomb*, Oxford, Centre for Governance of Artificial Intelligence, September.
- Ponce Del Castillo, A. (2021), "La stratégie numérique de l'Europe : centrée sur les personnes, sur les données ou sur les deux ?", *Bilan social de l'Union Européenne*.
- Radulov, N. (2019), "Artificial intelligence and security. Security 4.0", *International Scientific Journal – Security & Future*, Vol.3, n°1.
- Siegmann, C. ; Anderljung, M. (2022), *The Brussels Effect and Artificial Intelligence: How EU regulation will impact the global AI market*, Oxford, Centre for Governance of Artificial Intelligence, August.

- Smyrnaios, N. (2023), "Les GAFAM, entre emprise structurelle et crise d'hégémonie", Pouvoirs – Revue française d'Etudes constitutionnelles et politiques, n°185.
- UNICRI (2018), White paper Artificial Intelligence and Robotics for Law Enforcements, Torino.
- Viscusi, G. ; Collins, A. ; Florin, M.-V. (2020), "Governments strategic stance toward artificial intelligence: an interpretive display on Europe", in *ICEGOV '20: Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*, September 2020.
- Zuboff, S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York Public Affairs.