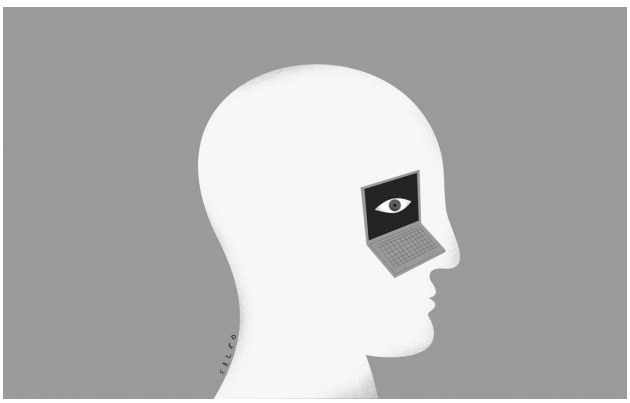
The threat to national security and private data collection of the state in the eyes of Human Rights

Romane Gielnik[1]



Drawing by *Carlos Alejandro Chang Falco*, Cuba.

In this article, it is debated on how the collection of individual's private data by the State affects Human Rights. The peculiar context in which intelligence took its place in our societies has created all its traits and aspects we have today. It has been developed in the age of the Cold War and the War on Terror, a very politically uncertain part of history, which led most governments to fear for their safety. Also, the simultaneous rise of the Digital Age, since the 1950s, nourished this common fright: a new, unknown and unmastered tool was being spread in the hands of all individuals. Two main issues were then confronting each other: the need to preserve the individuals' security as well as their right to privacy and others Human Rights. The interests seemed to oppose each other: to grant a total right to privacy to individuals rhymed with a lack of surveillance of the State on individuals and hence the inability to protect their citizens, when the collection of private state seemed to intrude the right to privacy and so weaken democracy, freedom of opinions and others. If the two notions are opposing, it does not, however, necessarily mean they are contradicting each other: norms should evolve according to the society they serve.

Introduction

In a recent case of 18 November 2021, at the Court of Justice of the European Union, the Advocate General *Manuel Campos Sanchez-Bordona* formulated the general principles of data collection and retention by the Member States: he held that „the general and indiscriminate retention of traffic and location data relating to electronic communications is permitted only in the event of a serious threat to national security" and added that „national legislation which requires electronic telecommunications undertakings to retain traffic data, on a general and indiscriminate basis in the context of an investigation into insider dealing or market manipulation and abuse, is contrary to EU law"[2]. Such principles have been held before in the European's case law, and are now considered as the basis for further development of legislation on the regard of collection and retention of data relating to electronic communications. However, nowadays, the States collect the data of their own citizens in the name of national security.

If spying is a very old method of getting information, global surveillance arose only around the late 1940s, and developed mainly in the context of the Cold War, and later on the rising of terrorism, with historical events such as the attack on the Twin Towers of the 11 September 2001. One of the first known international agreements on global surveillance is the UKUSA Agreement, which aims for cooperation in signal intelligence between its members, such as the United States, Canada, the United Kingdom and others. Officially enacted in 1946, the existence itself of the treaty was known to the public more than 50 years later, in 2005. A few years later a controversy arose about the treaty and the practice to which it led. The 2013 National Security Agency leaks of the United States of America accused members of the treaty

[1] The author is a student at the University of Lille, France, from the Bachelor of International and European Law, currently a member of the Erasmus+ program in the University of Wroclaw, Poland.

[2] Opinion in Joined Cases C-793/19 and C-794/19, in Case C-140/20, and in Joined Cases C-339/20 VD and C-397/20 SR.

to purposefully spy on each other's citizens so as to share information on their citizens.

On the one hand, personal data refers to any information that serves to identify an individual, whether directly or indirectly, such as a full name, scan of the iris of the eye, IP address or card number, such information is known as „identifiers". On the other hand, private data is the one that is not usually disclosed, in accordance with national legislation, because it is considered to be a part of the intimacy of the individual. Its collection by a State refers to the concept of mass surveillance, the indiscriminate monitoring of a population, mostly via the means of new technologies, such as a phone, surveillance camera footage, or the use of the Internet.

This concept is known for its controversial aspects: the concept itself of mass surveillance implies interference with the individual's right to privacy, and the potential further consequences on the freedoms of individuals, such as expression and protest (for the purpose of this work, the surveillance of known criminals will not be approached. This includes matters such as the collection of data in criminal cases, namely those aiming at legitimate prevention, investigation and detection or prosecution of criminal offences and the execution of adequate penalties). Lastly, national security refers to the prevention of all threats to the territorial integrity, the economic and ecological security, the physical safety of people, as long as there is social and political stability of the State. It can mean the prevention and protection against natural disasters, national defence via armed forces, digital security, health and prevention of criminal interference… or mass surveillance.

Mass surveillance developed in the objective to keep safe all human beings on the State's territory, which is why it gained strength in the Cold War and the early 2000s, as the world faced a rise of terrorist attacks. However, when such surveillance becomes so massive that most common individuals are spied on, it may cause damages to any democratic society. Indeed, the government is then able to restrict as it wishes the freedom of thought and political opinion, which breaches the right to privacy as a fundamental Human Right, via legal norms such as the European Convention on Human Rights in its article 8 „right to respect for private and family life, home and correspondence".

The complex choice of the use of mass surveillance is inherently tricky, and almost paradoxical. How can one choose between security or freedom? There must be an equilibrium that has to be found between the two notions that guarantees both on legal grounds, while answering to the new challenges of the Digital Age. In other words, the issue raised here must be understood as: „To what extent can a State collect private and personal data in the name of national security, without violating fundamental Human Rights?".

Surveillance rose in a peculiar context. In the last century, the world suffered from many interstate conflicts that grew alongside the development of the Digital Age, causing them both to naturally have a strong connection. However, this development led to paradoxical legal questions that are yet to be answered. This means that new threats arose, to which new means of defence and protection shall be developed as an adequate answer to this evolution. However, every progress opens a new legal field, in which legislation needs to be built: law must adapt to the reality of its contemporary world, which includes the protection of Human Rights in all aspects. In the end, these correlated evolutions answer each other very closely: if one makes a move, the other will too, in the same way of a „question/answer" game mechanism. There needs to be a balance that guarantees both safety and freedom of the individual, according to the various interests and values of a State, as both notions may be opposites, but not necessarily contrary to each other, which may lead to consider a possible coexistence of both of them.

The rise of surveillance in a peculiar context

The ways of attacking a State were completely changed during the 20th century, which led surveillance to rise in a very unique context in the world's history, torn apart between a new growing threat to national security and the digital revolution.

1. The origins of a growing threat to national security

The 20th century is known for its numerous wars all across the world that marked the whole world's history. Besides the three main conflicts (First and Second World Wars and the Cold War), multiple other events happened, such as the Third Afghan War (1919), the Russian, Spanish and Irish Civil Wars (respectively 1917–1922, 1936–1939 and 1922–1923) and tens onward. Since then, the world has been constantly under worldwide conflicts. Even if the Gulf War (1990–1991) happened on Iraq and Kuwait territory, the United Nations took part of the conflict mainly by imposing measures such as trade embargo and military coalition of millions of individuals from 32 countries prepared in case diplomacy and would not be able to solve the conflict.

The implication of States to the conflict became usual, and even the new normality. Nowadays, we expect those States, mainly great powers, to try and regulate conflicts. In the recent events between Ukraine and Russia, countries such as the United States of America and France have made official declarations: the French president *Emmanuel Macron* officially affirmed his support to the Ukrainian

people, and the Commander in Chief of the US military, *Mark Milley*, also spoke about the conflict on the same day (28 February 2022).

This new perspective on interstate conflicts grew from a very peculiar conflict that remodelled the concept of war itself: the Cold War. After the end of the Second World War, a whole new way to deal with an international conflict arose, in which the victory was not given by military forces and weapons, but by information and strategy. If surveillance and spying are very ancient methods to mankind, it was taken to a whole new level in the second half of the 20th century.

Intelligence gathering became a priority for both the Soviet Union (Eastern Bloc) and the United States (Western Allies), as a heritage from the nuclear espionage, during the Second World War. Nuclear weapons, considered as one of the most important of all State secrets, were and still are widely coveted. As an illustration, the Manhattan Project was a cooperation between the Allied States, the United States, the United Kingdom and Canada, aiming at developing the nuclear weapon together. The said „atomic spies" would gather information for the sake of the Soviet Union, one of which is known today as *Klaus Fuchs*, a physicist responsible for theorical calculations to both the early nuclear weapon and the hydrogen bomb.

Espionage between States kept rising and took a major place in the States' missions. Nuclear espionage, communications interception and military strategy became the centre of the American Central Intelligence Agency, known as the CIA and the Soviet Komitet Gossoudarstvennoï Bezopasnosti (Committee for the State's Security), known as the KGB.

After the fall of the Soviet Union at the end of the 1980s, the Cold War ended, but States kept their habits of surveillance. A few years later, the September 11 attacks of 2001 turned the world upside down. In the spawn of a single day, the terrorist organisation al-Qaeda planned four attacks on the American ground. Four planes were hijacked mid-air. Two hit the Twin Towers in New York City, a busy working area where thousands of people died and traumatised the whole country. Another plane hit the Pentagon, American headquarters of the US military and defence. The last one was aiming to crash in Washington D.C., the Capital city of the United States and the location of the White House. However, the passengers revolted and it crashed in a field in Pennsylvania. The event is still remembered today as a collective trauma to all Americans that witnessed the events: it was aiming at the destruction of all main aspects of the State: economic, political and military.

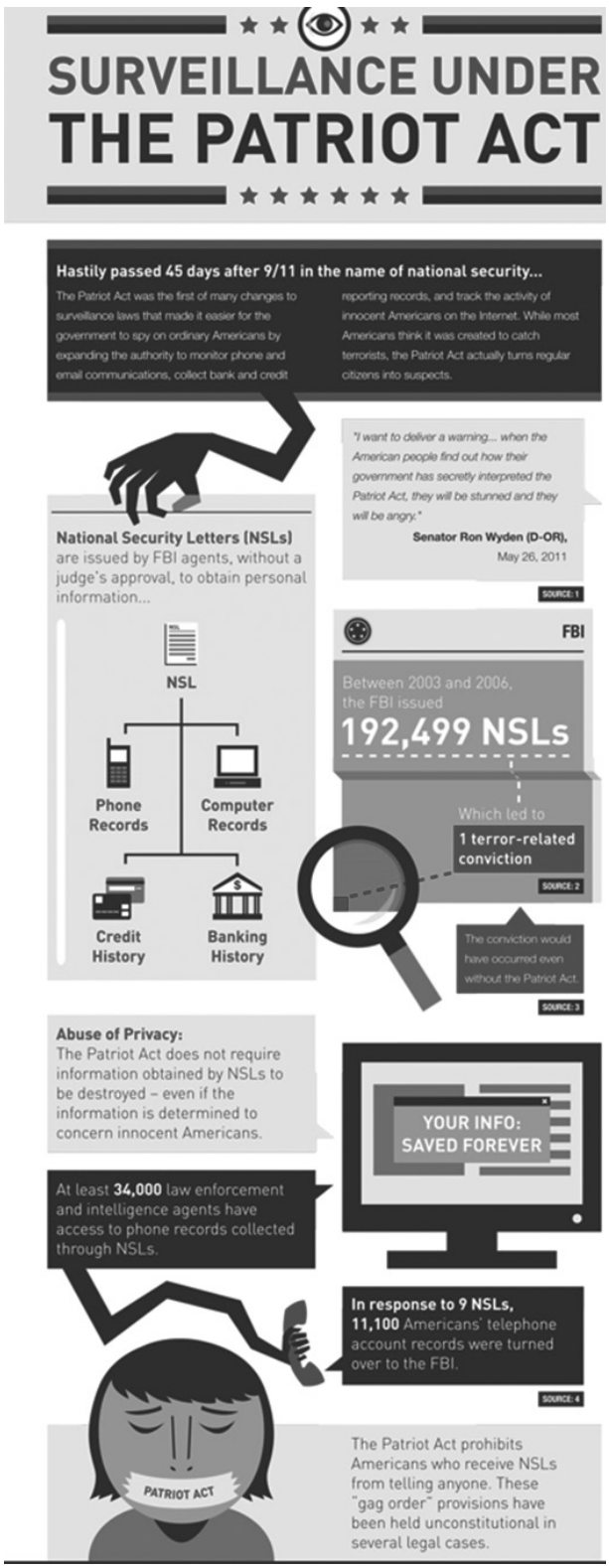
It was the first time in History that the United States of America were attacked on their ground by an outsider, as the only previous combat happened in the Civil War. The day before, the Americans believed they were absolutely safe on their grounds and would not have felt threatened in any way by an attack on their territory, contrary to Europeans who knew hundreds of wars on their grounds, including both World Wars. Many worries and questions were raised then, mainly about security and privacy. As a response, a „War on Terror" has been declared, which led the American defence to build a new program on protection of civilians and destruction of terrorism. The immigration policy was reimagined, and the fear that grew in everyone's heart led to events of racial profiling and hate crimes towards the Arabic and Muslim communities.

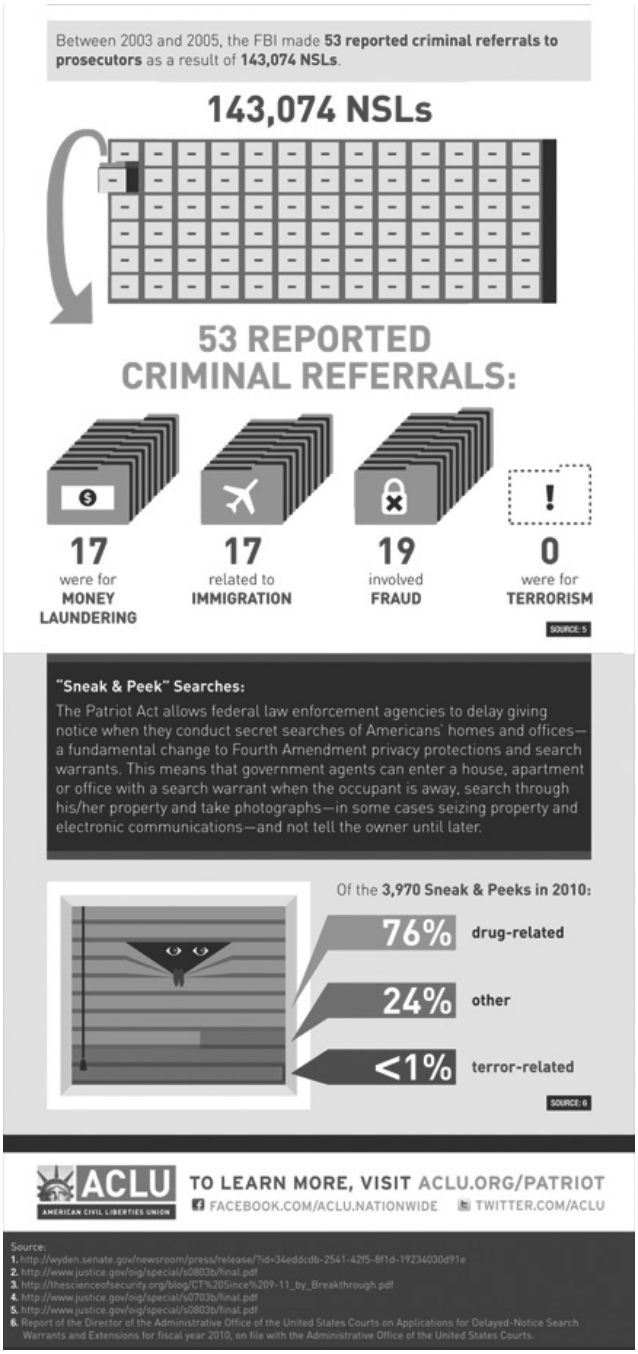
The Act of public law of 26 October 2001, „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism", known as the USA Patriot Act of 2001, has been the legal response to the events of September 11. It amended the Foreign Intelligence Surveillance Act of 1978 and added various new provisions.

Many changes were made, like reinforcement of criminal laws against terrorism to be more strict, but also „enhanced surveillance procedures (Title II)", „improved intelligence (Title IX)". The Second Title is meant to give authority to „intercept wire, oral, and electronic communications relating to terrorism" for the purpose of investigations and/or prosecution.

The Patriot Act was voted by the American government to change surveillance laws with the aim to spy on ordinary Americans in the name of national security. Surveillance agencies could then spy on phone and email communications, unnoticed, in the daily lives of their own citizens, as much as many other intrusions of privacy. The use of National Security Letters (or NSLs) was developed: agents of the Federal Bureau of Investigation (or the FBI) could obtain and store anyone's personal information with no requirement of a judge's approval beforehand. In three years, from 2003, almost 200,000 were issued, and only one led to a conviction in relation with terrorism, for which the Patriot Act has not been particularly useful (see below: Drawing No 1).

Drawing No 1: Surveillance under the PATRIOT Act.





Source: Surveillance under the PATRIOT Act, ACLU.

Some temporary programs have been very controversial until their disappearance, such as the" business records" provision, which refers to Section 215, „Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations". It amends the Title V of the Foreign Intelligence Surveillance Act of 1978 and states by inserting: „The Director of the Federal Bureau of Investigation (...) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents and other items) for an investigation to protect against international terrorism (...)".

In practice, it gives a large margin for the government to ask for anyone that might be involved in terrorist affairs. In 2013, a leakage of documents showed that the government had been collecting phone records of anyone who had a functioning phone, by all companies, under Section 215. *Edward Snowden*, a former computer intelligence consultant, was the source of that enormous leakage of the National Security Agency's documents. Later on, the United States Court of Appeals for the Ninth Circuit ruled that data collection by the NSA, such as exposed by *Edward Snowden*, was illegal on the grounds of the Foreign Intelligence Surveillance Act, and possibly unconstitutional (2 September 2020).

All of those practises are closely related to the recent occurrence of the digital revolution and the new world of possibilities it offers.

2. The relationship of surveillance to the digital revolution

Alongside the movement times of the Cold War and the „War on Terror", the digital revolution also re-shaped the world. With the first computer available to the public being commercialised in 1951 and the development of the Internet's ancestor, Apranet, about twenty years later, the use of digital technology expanded exponentially in both civilian and military aspects, until it became a tool of all our daily tasks. The United Nations specialised agency for ICTs (Information and Communication Technologies) states that about 63% of the world population are connected to the Internet, which represents about 5 billion people.

If there are many ways for the Intelligence agencies of the world to spy on anyone, most of them are via electronic devices and the Internet. Postal services, aerial surveillance, biometric surveillance, infiltration of human operatives, satellite imagery… but mostly computer or telephone surveillance, cameras, social network analysis, data mining and profiling, geolocation devices… are now a part of everyone's daily life.

Since their early years, digital technologies have become the most important source of information for most of us. The Internet is meant to be accessible and easy to use, to all generations. The older generations can use them (if their grandchildren teach them a little), and even toddlers (even though doctors do not recommend it): any member of society has access to it, and the network covers most of the surface of the habitable lands of the world. Such technologies are used daily: when you order food at a restaurant, when you buy a bus or tram ticket, when you call family members or friends, when you play online games, work or study, and even at school.

These technologies have developed mainly during Cold War and have never stopped evolving since then. Military resources are now digitised as well, as much as the Intelligence agencies. In the second half of the 1950s, even before the use of e-mails and computers was democratised, an abuse of surveillance was committed by both the CIA and the FBI, via postal services. The HTLINGUAL program ran until 1973, in which every information outside of a package or envelope was recorded, and allowed to open mails without warrant to read its contents. More than 215,000 pieces of mail were opened this way.

Nowadays, the access to such data has become even easier. Indeed, digital technologies provide opportunities to „hack" the common individual's data, such as phone or computer records or even credit and banking history. As an illustration, the hacker *Kevin D. Mitnick* explains that all web mail is „cloud based", which means that, for instance, every email received via Gmail has a copy on Google servers and can be inspected by the hosting company. The official purpose of such measures is to filter out malware. But this way, we, citizens, have no clue why and which emails are read, and neither on what criteria, by the surveillance programs that have a right to claim their data to such companies.

Initially, such data collections via digital tools were meant to prevent criminal activities and protect civilians. It is how programs such as Section 215 of the USA PATRIOT Act expanded their abilities, using the large ocean of data that the Internet is. Indeed, when the common citizen uses online means, they will use online payment, online communication networks and social media such as Twitter, Instagram, Facebook and much more. The digital age allows an easier access to data, but also an easier storage and analysis of such data. Bots can be programmed to pursue a certain mission, and so, less work is required for better results, which facilitate the wide spreading of surveillance to common citizens: intelligence agencies do not have to limit themselves to the known criminal organisations anymore.

Bots are automated software programs: they can achieve repetitive tasks, or predefined tasks according to how their particular algorithm has been coded. It is estimated that about a half of the current activities online are executed by bots. They are used by a wide variety of actors: individuals, companies, hackers, but also for surveillance purposes. Surveillance and security robots in civilian environments can be used for many purposes. They monitor the behaviour, the changes of activities, the habits and all possible information. They can be programmed to execute tasks such as target detection, to keep an eye on an individual, via an automatic system of data collection, filtering and storage.

It can recognise facial features by tracking facial landmark points from any angle, and any facial expression, even if parts of the face are hidden. As an illustration, the Chinese government makes use of this technology to keep a close eye

on its citizens via Closed-Circuit Television, which are cameras disposed all around public spaces, like streets, parks, supermarkets and more. By 2018, it was estimated that over 200,000,0000 of such cameras had been installed all over the country, of which a great majority have been installed by the government. It has been recognised that a camera can look for a thousand people at a time, yet Artificial Intelligence experts are working to constantly improve those performances.

全国信标委生物特征识别分技术委, which translates into the National Information Security Standardisation Technical Committee, is meant to enforce mandatory standards for facial recognition in the country. Every person in China in possession of a mobile phone with a registered SIM card has to submit to facial recognition scans, to certify the identity of the holder, which makes them largely easier to track.

A Chinese teacher, *Guo Bing*, employed at the Zhejiang Sci-Tech University, filed what is thought to be the first lawsuit against such practises, as his private data was taken without his consent at Hangzhou safari park, using such a method of facial scanning. Relatedly, the Human Rights activists *Kenneth Roth* stated on a Twitter post, on 1 December 2019 that „China further extends its dystopian surveillance state", which refers to the system of social score based on your actions and the government's appreciation: buying alcohol or criticising the government makes you lose points, which can lead to a ban from travel or public shame, and beneficial actions would be rewarded, like participating in charity events.

Cutting edge technologies reinforces the power of surveillance of a State. By reducing the anonymity of people on the Internet, by legally forcing individuals to register their real names when creating accounts online, the artificial intelligence and bots could easily trace individuals' activities and establish profiles.

Skynet is a surveillance system created in 2005, yet revealed to the public in 2013. At that time, 20,000,000 cameras were already installed in the streets of China's cities all over the country. The official purpose is to track criminals in a very short time, with cameras being able to recognise anyone in a very short notice, faster than any human intelligence service could ever do. The idea here is to protect nationals, however the use of such technologies have been revealed to go further than tracking of wanted criminals.

Abuses have been revealed: the region of Xinjiang, North West of the country, is the homeland of the Uyghurs community, a Muslim ethnic group. They are forced to give out their biometric data to the State, which includes fingerprints, DNA samples, and voice samples, to allow the government to track them without restriction at any time. Simple actions like growing a beard can then lead them to be interrogated by police and even being put in prison camps.

Other tracking technologies are also used for the purposes of mass surveillance by the Chinese government. Legal norms censor international applications and social media, and force the citizens to choose the „Chinese versions" of those applications. For example, the trendiest social network as of today is „Tik Tok", developed by the Chinese government itself, but for non-citizens. Their citizens shall use 抖音短视频 (also known as „Douyin"), an application that can be downloaded only if you are permanently geolocated in China. It aims to restrict the foreign influences and users, and allows the government to put into place means of data collection and censorship for the State's benefit. Other western applications like Facebook, What'sApp or Uber are being replaced by „WeChat" (that also can serve as a banking service), which facilitates surveillance by the State by gathering all information of individuals in one single application.

What even more facilitates this process for all States is the concept of metadata. Metadata is information of specific features: it is information that provides information for another data. It can be titles of articles, keywords, summaries of e-books, statistical, administrative or legal data. That information create links, and may even reveal new data that has not been directly put online.

The European Court of Justice, in its jurisprudence of „Tele2 Sverige" of 21 December 2016, held that metadata as sensitive information as the content of messages and mails in the perspective of guaranteeing freedoms and rights to the European citizens, mainly in the eye of the right to privacy. They have been listed as „data that makes it possible to trace and identify the source of communication and its destination, to determine the date, time, duration and type of communication, the users' communication material, as well as locate mobile communication equipment". This makes massive metadata collection illegal for commercial purposes and the establishment of highly detailed profiles of individuals, but also state's surveillance collection, even in regard to anti-terrorism protection policies.

That is where a strange idea arises: the protection offered by States to citizens may take away their freedoms, even if the State itself is in charge to guarantee them.

The paradoxical choice between security and freedoms

That highly developed information creates moral and ethical difficulties that are yet to be solved. One the one hand, there is a need to protect the individual from any threat, counterbalanced on the other hand by the need to guarantee Human Rights to all individuals.

1. The need to protect individuals from this threat

The notion of a State is not natural to mankind. The concept has been invented quite recently, when humans started to grow in bigger societies. The first kind of „human" is believed to arrive on earth about 7 million years ago. If our knowledge of their lifestyle is quite limited, since then to the first men of Neandertal (about 300,000 ago), we know that we have always been in groups, living in families of various sizes, but never alone – at least purposefully. Humans gathered and organised themselves in hierarchies, until the first human civilisations, allowed by knowledges such as craft, writing, agriculture, and livestock, in the Fertile Crescent of the Middle-East. Civilisations such as Egyptians were born there and then, and structured themselves in the first systems that would fit our modern concept of a „State".

States were made for a purpose. The French philosopher, *Jean-Jacques Rousseau*, wrote his ideas on the origins of a State in his work „Du contrat social ou Principes du droit politique" in 1762. He elaborates this idea that men, to protect themselves and improve their living conditions, have agreed to give up a part of their natural freedoms to a man, superior to all else, in exchange for safety, via „pacte social", an agreement. However, he insists that all should be protected by others, and so give up the freedom that is harmful to others, and only those. It refers, for instance, to the liberty to kill: prehistoric men, without laws and courts to control their actions, would be free to kill someone for their personal gain, and there would be no justice done for his actions: just a never-ending circle of revenge. The Social Contract is the common agreement to give up on this old model of revenge to become a fair and pacifist society within its members.

This abandonment of the idea of „might makes right" (or kraterocratie, from the Ancient Greek, meaning that power belongs to the strong ones), led to the current duties of States to protect citizens. But the protection of citizens means to guarantee their rights: if we cannot kill, it is to guarantee the right to life. If we cannot steal, it is to guarantee the right of property. If we cannot discriminate, it is to guarantee equality.

Modern societies such as ours have evolved a lot since those first civilisations. The possibilities to attack someone, to violate someone else's rights have become wider, notably since the digital revolution. Governments have to expand their protection to the digital world: it is unimaginable that a State would have a criminal policy, but no laws concerning cyber criminality. The Internet is a shared space, in a similar way that a street is, in this regard. For instance, in a country where drugs are illegal, it should not be possible to buy any online. Otherwise, dealers and clients would just need to code an online shop to go around all the criminal laws. This would imply that any crime is not punishable if committed online, which would not guarantee rights of the individual at its fullest, causing the State to automatically fail at its mission of protection of civilians.

It is following this objective that the European Union adopted a Regulation (the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC „Data Protection Directive"), known as the General Data Protection Regulation 2016/679, or GDPR, implemented in 2018. Its first article states the subject-matter and objectives of the regulation: „1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. 2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. 3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data".

It hence recognises the Digital tools as potentially dangerous, and the necessity of a legal framework so as to guarantee the citizen's free and fair use of those means. The European Union aims at protecting citizens from online criminality, but also to protect the individual's personal data. Data processing requires the individual's explicit and aware consent, unless it is in their vital interests, or the compliance with legal obligations, for instance.

As an illustration, medical data is considered to be one of the sensitive personal information that should not be forced to be revealed without explicit and informed consent. However, during the Covid pandemic, some countries required a proof of a negative PCR test or vaccine against the disease. As an illustration, the French government established limitations on the access to some places available to the public, such as cinemas, museums, shops or restaurants. „Le pass sanitaire" was a QR-code given after being vaccinated in a specialised establishment that would be valid after two injections, currently turning into three injections, of the vaccine. Implemented in June 2021 and still in place up to date, this was a very controversial measure. Citizens are required to register their QR-code into their phone via an application developed by the government, „Tous Anti-Covid" (which translates into „together against covid"). Then, anytime they enter a public place requiring the presentation of the vaccinal pass, they have to show their QR-code at the entrance, where it would have been checked by a security guard, or in some cases an employer.

The obligation to disclose such personal data has been justified as a temporary measure that is not meant to last in time, and serves national security as it aims at preserving public health. It allows the government to enforce its meas-

ures. In the controversy that it leads, the resistance to such measures, even in the name of national health, security, and public order, comes from the highly sensitive nature of the data. Other than just disclosing your personal information, you also give out your position, where you were and with whom, as you register your QR-code that contains all that information.

The State's objectives are to preserve national integrity, safety of its citizens, and its fundamental interests. For a State to last in time, it needs tranquillity and trust between the government and the individuals. Covering the nation's interests online is just as fundamental to guarantee those two feelings as any other policy. For a national unity, there is an absolute need for the State to protect citizens in all aspects of their lives. As individuals spend more and more time online, as much as share more and more data online, sometimes without even realising it, a State cannot be forbidden to have a presence online for defensive and protective means, this would simply not be adapted to our times.

States must have a possibility to keep an eye on what is happening online, as much as to react to such things. The question, however, is where the limit of this ability should be. When is it too much freedom and too little security? And, on the other hand, when is it too much security and too little freedom?

To grant effective protection, new rights were granted to the individuals making use of digital technologies. The fundamental rights of data subject has been recognised as such: the right to access to information, the right to access to the data itself, the right to rectification of your data, the right to be forgotten (which implies the right to delete information about yourself), and the right to withdraw consent at any moment. To guarantee that protection does not overrule freedoms, these new rights have to be guaranteed by the State, as any other right.

2. The need to guarantee the individual's Human Rights

The European Court of Justice has shown opposition to the mass collection and storage of data from online connections and phone use by States. On 6 October 2020, it held such a decision, rejecting the possibility for States to require Internet Service Providers, or ISPs, to give out the data and metadata of their clients, even for purposes of justice and surveillance. More precisely, it was held that States could not impose „une obligation généralisée et indifférenciée". This means that it is not possible to imagine a general legal norm imposing all ISPs to share their data to the States at all times, from all of their clients and all of their communications.

It was deemed that measures such as those taken by France, Belgium or the United Kingdom (that latter still being a member of the European Union back then) in the context of their anti-terrorism policies were contrary to European law. The collection and storage of such sensitive information have to be limited and based on legitimate interests: all citizens cannot have their information collected at once, according to the General Advocate *Manuel Campos Sanchez-Bordona*. Targeted and precise surveillance does not fall under the scope of the restrictions imposed by the State. They attempted to contest this decision, on the basis that according to the Treaty of the European Union, national security is the competence of Member States and Member States only: it is exclusive and the European Union should not be entitled to restrict its possibilities.

In a more recent opinion of 18 November 2021, the same Advocate General, *Manuel Campos Sanchez-Borbona*, added that the „general and indiscriminate retention of traffic and location data relating to electronic communications is permitted only in the event of a serious threat to national security". The element of a serious threat to national security is recognised as the only possible justification, as a strict condition, to mass surveillance of individuals by the State. It would be possible to exercise such measures in cases where it is absolutely required so as to guarantee the safety of the individuals, in which case it is recognised as a proportionate and adequate response to the threat.

It cannot be understood that this scope widens, as it implies interference with basic Human Rights guaranteed by most Human Rights Charters across the World, notably the right to privacy. The consequences on the deprivation of the right to privacy, guaranteed by article 8 of the European Charter on Human Rights, has consequences on other Human Rights. They are fundamentally related to each other, and the loss of one may result in the loss of all. In this case, it might limit the rights to freedom of expression and opinion, which impacts democracy as much as the rule of law itself, and their safeguarding.

Murray Gleeson, a former Chief of Justice in Australia, defined what makes data private. He established a simple test to determine any information as such: „The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private". Hence, if it is generally accepted that the information is usually not shared with others, except for close relatives or friends, the data must be considered and treated as private. People might want to keep their data private for many reasons: the need for intimacy, the social pressure that may ensue, or the fear that such data may be used against oneself.

In the case of collection by a State, the use against oneself would be the main scare for individuals. One of psychology's principles, known as the Observer Effect, explains that there is a „self-editing effect". It implies that the individual

would automatically filter their words if they are aware of a possibility to be recorded by a State, even if the said State is not actively doing so. This tends to be even more noticeable when the said individual has political or cultural opinions that vary from the usual norm amongst the citizens, and the State policies. As an illustration, we may use the anachronist example of the creation of democracy. If *Cleisthenes* was being potentially watched by a conservative intelligence system, he may not have reformed the political regime of Athens in the year 507 B.C., and the demokratia would never have been implemented. Society would not have been able to evolve, and in that scenario, we probably would not live in a democracy today.

In those cases, misuse of private data may be the source of worry. In a State like China, citizens are taking disproportionate risks by criticising the government. They fear for their life and restrain their will to speak up about their opinions, beliefs, in case they might be in discordance with the government policies, as it may detain that information to sentence every attempt to contradict the measures in place. This limits the diversity of ideas in a society, and causes the citizens, mostly younger children, to automatically agree with the government by lack of exposure to new and different ideas. How can Chinese people reject the exponential development of cameras equipped with artificial intelligence if they have been told that it helps with keeping the country safe, but have never been told what risks might be the cause of it? What downsides are to be expected? In the long run, it limits the possibility itself to think for themselves, to develop a very own and personal vision, but conforms all individuals into one path of thought.

Article 8 of the Convention of Human Right, on the right to respect for private and family life, states that „1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

These framed limitations of article 8 are closely related to the need for protection of private data: self-determination of the use of our personal information is the key to preserving all rights required in a democratic society led by the rule of law, which the State is bound to safeguard. The European Court of Human Rights held in two General Court jurisprudences, *Centrum för rättvisa v. Sweden* 2021 and *Big Brother Watch and Other v. The United Kingdom* 2021, that the existence of secret data surveillance deprives of the rights guaranteed by article 8 as it is impossible for the individual to challenge the act and they are not aware of what can be performed with their own data. The mere existence of such a policy can lead to a violation of the article in certain conditions as stated in *Roman Zakharov v. Russia* 2015 (§ 171–172). There is a need for supervision of the relevant national judicial authorities, to prevent abuses and misuses. National authorities cannot have full and incontestable discretion in determining what system of surveillance is required, and its extent.

Surveillance is legal and tolerable as long as it is strictly necessary to preserve democratic institutions, and remedies shall be available to sentence abuse and misuse of surveillance. In the case of *Weber and Saravia v. Germany*, the Court held that data must be „used only for the purpose which had justified their collection" (§ 150) and that „in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse (...). This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law" (§ 106). In this regard, the Court found to be in violation of the article regarding the recording of a conversation by a long distance radio device during a police operation without procedural safeguards[3] or the systematic collection of data of security services targeted on particular individuals even in public places[4].

Even if article 8 of the Convention is the most obvious regarding the risks to Human Rights caused by mass surveillance, it is far from the only one: for instance, Article 6, on fair trial, also reveals potential limits to the possibility of mass surveillance. In *Lopez Ribalda and Others v. Spain* 2019, the Grand Chamber of the European Court of Human Rights held that the use of evidence based on data obtained in violation of article 8 and/or in violation of domestic law, the trial must be considered as unfair and breaching article 6 of the convention, as it may interfere with the defence rights to the parties, and the opportunity to contest the authenticity of the evidence has to be ensured as well. Nuances shall be brought, as evidence rules for civil and criminal proceedings vary[5].

The complexity of the application of mass surveillance is its paradoxical consequences: it opposes the security to freedom, two fundamental elements to a fair and safe democratic

[3] *Bykov v. Russia 2009*.
[4] *Peck v. United Kingdom 2003*.
[5] See: Article 6 of the European Convention on Human Rights.

society, as neither of them shall be undertaken by the other. It enhances a need to search for balance, an equilibrium that could guarantee both to all individuals.

The search for balance between security and freedom

In the context of mass surveillance, security and freedom have a rather conflictual relationship. First, it is necessary to understand the various interests that justify security and/or freedom as fundamental in our societies. Secondly, there is the need to nuance an apparent opposition of both concepts that seems to counterbalance each other, as if a choice had to be made when our democratic societies need them both as much. We shall aim at the coexistence of those two concepts, even though they seem opposites, they do not have to be contradicting each other.

1. A divergence of interests to protect

As *Arnold Wolfers* said in 1952, „the term 'security' covers a range of goals so wide that highly divergent policies can be interpreted as policies of security". Indeed, the word security may imply the protection by the State of individuals, institutions, economic powers, territorial integrity… All threats imaginable must be ward off by the State: it is nowadays the State's role to keep individuals safe from murder, discrimination, food security, but also Human Rights violation, terrorist attacks, cybercrime and so much more.

This may be done via the American National Security Act of 1947, the German White Papers („Zur Sicherheit der Bundesrepublik Deutschland und zur Entwicklung der Bundeswehr"), the Chinese White Papers, such as the one from 2019 which reinforces its strategic partnership with Russia, the French White Papers of 1972 which aims at reducing the proliferation of nuclear weapons, or even the Japanese with constitutional norms and the National Defence Program Guidelines.

All States have policies of national security and defence. However, according to their very own values, expectations, means and beliefs, those policies may have their priorities at highly divergent points. Indeed, due to their particular culture and history, all States have different problems to face while protecting their country, and this applies just as much to cybersecurity and intelligence. During the 2000s, countries such as the United Kingdom, the United States of America or France had their national security centred on the fight against terrorism, while Japan was more focused on the area of the Pacific region of Asia, where tenses were rising in China on internal divisions such as the issues of Taiwan and Xinjiang.

States have different characteristics, which have been analysed in *Buzan's* 'People, States and Fear', book of 1991. The author focuses his work on two fundamental factors: the power of a State, notably its military abilities in international conflicts, and its socio-political cohesion, which refers to the nation's stability and unity of its people. This model shows that a State with weaker military forces and low social cohesion will be more vulnerable to most types of threats. A State with a weak military power will only be vulnerable to international threats and invasions, while a State with no socio-political cohesion will be the most vulnerable to internal threats such as civil revolts. All those States will not have the same idea of potential threats, and of national security and measures to take. In the eyes of mass surveillance, this implies diverse possible uses of such measures, as much as different needs and levels of implications demanded by the States (see below: Tables No. 1 and 2).

Table 1. Vulnerabilities and Types of States (taken from People, States, and Fear (1991))

Weak		Socio-political Cohesion	
		Strong	
Power	Weak	Highly vulnerable to most types of threats	Particularly vulnerable to military threats
	Strong	Particularly vulnerable to political threats	Relatively invulnerable to most types of threat (less inclined to characterize issues as military)

Table 2. Cyber Vulnerabilities and Types of States

Weak		Socio-political Cohesion	
		Strong	
Power	Weak	De-stabilizing political actions in cyberspace, attacks on Internet infrastructure, criminal activities	DDOS and other major attacks on critical infrastructure*
	Strong	De-stabilizing political actions in cyberspace	Criminal activities in cyberspace

*A distributed denial of service attack, or DDOS, occurs when many computers, usually surreptitiously controlled, are used to inundate a web server with requests and cause it to become overwhelmed to the point that service is denied.

Source: Tables extracted from *B. Buzan*, People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era, 1991.

The first type of a State will be worried about most types of threats that may be foreseeable in cyberspace. The second type will mostly be worried on issues of attacks on the Internet infrastructure, international terrorism and interstate conflicts, while the third will be more focused on politically destabilizing forums, for instance. Surveillance may be used as a tool to protect from each of those threats, by making different uses of the same abilities intelligence agencies have. The objective leading mass surveillance measures will be strongly connected to the extent and consequences on liberties of such surveillance.

This emphasises that even if the security brought by mass surveillance may infringe fundamental liberties and freedoms and even Human Rights, there can be hundreds of ways to link those two notions, and how they interact.

2. The coexistence of opposite but not contradicting ideas

As elaborated earlier, the notions of freedom and security are conflictual when it comes to mass surveillance. In this context, data collection interferes with freedoms it is trying to protect. Mass surveillance and data collection by the States aims at reinforcing national security and guaranteeing the safety of each individual. On the other hand, not permitting the State to have such surveillance abilities would not guarantee everyone's security, even if that would not interfere with freedoms.

Those impacts will mainly depend on the means and ways of mass surveillance, data collection and storage. The United States of America and China both have mass surveillance programs. However, it does not have the same consequences in both countries: in China, each individual's single actions are evaluated and analysed, and so every word they say may be prejudicial to them which leads to a fall of the liberties of expression, freedom of opinion and rights to a private life. In America, mass surveillance collects a lot of data and mostly metadata, in the purpose of finding actual threats to the nation, via very intrusive means. This reveals that even if this violates the right to privacy, it does not in all cases lead to the fall of democracy and liberty of thought.

The concepts of security and freedom do not have to be opposed to each other. Today, in the context of mass surveillance, they surely are. However, it might be possible to think of a method of surveillance that would not infringe liberties at all, including the right to privacy. We have to keep in mind that most measures in western countries were taken in the heat of the War on Terror, mostly as emergency measures and responses to the attacks of al-Qaeda and other such organisations: the USA PATRIOT Act 2001 was adopted just a few weeks after the events of September 11.

In all of history of humanity, first steps have always been halting and perfectible. The mass surveillance measures were taken in the urgency of a peculiar context and the sudden rise of terrorism, interstate conflicts and digital revolution. All those new threats and tools were still an unknown field, and to predict the consequences of such new actions may have been a real challenge.

However, today might be the time for a „post-project analysis", the time to reconsider the actions taken as much as their consequences, notably on Human Rights. To re-think previously taken measures and adapt them in a more rational way, with a deeper analysis of what it costs and what it allows. Nowadays, we have the hindsight that no one had thirty to twenty years ago. We have more concrete ideas of how digital tools may be used and their consequences on health, security, and liberties[6].

Security does not have to mean we give up on Human Rights. As *Jean-Jacques Rousseau* meant it, the role of the State is to bring security to the individuals, because safety is what allows them to be free. Inherently, security is a condition to liberty, and should not enslave it. The problem is not that mass surveillance keeps us safe, it is that the ways and the tools used in the policies of mass surveillance sacrifice liberties and human rights in the name of national security. This, however, does not mean coexistence is not possible at all: just not on our modern and current use of these tools. There are other ways to protect that we may use instead.

Conclusion

We may imagine a close future in which the States would gather and discuss those issues, and work together in the aim of mass surveillance and its current effects on Human Rights. A State has to protect its citizens from threats, even online. Rights and obligations shall coexist in cyberspace so as to ensure Human Rights, but without going into extreme ways that would cost the loss of Human Rights as well.

Here, there is a question of balance of values and considerations. New legal norms and regulations shall be taken in the light of the hindsight we now have. It is possible to keep an eye on people without taking away their right to privacy and other liberties away from them.

Surveillance of population may be possible without storing huge amounts of data and metadata to sort out information in a more intelligent and balanced way that would

[6] *P. Toomey, A. Gorski*, The Privacy Lesson of 9/11: Mass Surveillance is Not the Way Forward, ACLU 2021: „By reining in mass surveillance, Congress can begin the process of righting the privacy harms of the last twenty years. And looking toward the future, Congress can help ensure that the next generation of Americans are able to speak and associate freely, without fear of unwarranted government scrutiny".

guarantee all Human Rights and security at the same time. Working methods of intelligence agencies have to be revised in that perspective so as to ensure a safe world for all, while preserving both State's and individual's interests.

The main obstacle would be the compliance of the States, but all great changes in History came step by step. Every State has a unique policy and unique interests to defend as well, and so a generalised movement would require a lot of work of understanding of each other and communication, in the abstract of all political or diplomatic tenses there might be. Such great compliance has been seen before, notably with the establishment and recognition of the United Nations: it is not impossible when common interests are shared, such as global and stable peace. Change, even for the better, requires work and dedication. It is a progressive mechanism, an action for the future.

Keywords: National Security, Digital Age, Private Data, Surveillance, Human Rights, Privacy, Democracy.