INTERNATIONAL JOURNAL OF **DIGITAL AND DATA LAW**

REVUE INTERNATIONALE DE DROIT **DES DONNÉES ET DU NUMÉRIQUE**

ISSN 2553-6893

IMODEV
LES ÉDITIONS

Vol. 8 - 2022

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6893

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article n'engagent que leur auteur.

The statements published in this article are the sole responsibility of the author.

À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV. Enfin, associée de BeRecht Avocats, elle est avocate au barreau de Paris et médiateure professionnelle agréée par le CNMA.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Fondateur et associé de BeRecht Avocats, il est avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons_CC-**BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV. Partner at BeRecht Avocats, she is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-**BY-NC-ND**:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

THE INVISIBLE MAN IN THE DIGITAL AGE: FROM MYTH TO REALITY

by **François VIANGALLI,** Associate Professor, University Grenoble-Alpes, CESICE Grenoble, Cybersecurity Institute.

The purpose of this work is to put a question mark against the legitimacy of a hypothetical *Right to be invisible* in the digital world. It expounds the origin of such a discussion, its relevance and the specific reply it should, according to us, be given.

The invisibility has long captured the imagination of men. From Plato to Wells, through to Tolkien, no philosophy, literature or mythology has failed to consider the topic. Literary phantasm or pinnacle of the art of war, the invisibility is a philosophical myth as well as a tactical goal. In ancient times, before the digital age, the invisibility was mostly looked upon as more allegoric than realistic. This situation could change today, given our contemporary technologies, for two reasons. The first reason is that certain digital tools allow the skilful user to hide his traces on the network. If it is extremely difficult to remain physically invisible in the real world, in the digital world, it is not[1]. The second reason is that the scope of vision of the digital technology overpasses this of all previous technologies mankind ever wielded. In the Roman Empire, the Emperor himself could not know accurately what people felt like in the entire Empire and even in Rome, nor what were the consumption patterns of the population. No personal data were collected the way we know. Two thousand years later, things were still the same, just before the 2.0 web era. In order to know the opinion and the state of the country, Governments and private companies recruited researchers practicing real immersion in the social ambient they had to analyse, keeping record of habits and customs of the citizens. This situation has changed. Data collection and analysis have given the companies of the digital economy a power to observe, seek out and analyse what people do, think and say. The visual field has been extended prodigiously. If Bettelheim had prophesied the decline of privacy at the end of the 60's[2], no one could have anticipated privacy would become nowadays so vital, due to the observation we are all under and the protection we subsequently need[3].

Internet characteristics has led it to such an extended visual field, that entirely renews the question of invisibility.

[1] For instance, the *I2P* information network is explicitly defined by its conceptors as the project of the invisible Internet: www.geti2p.net.

[2] B. BETTELHEIM, "The Right to Privacy is a Myth", *Saturday Evening Post*, July 27th, 1968.

[3] See our 'Interview with Viktor Mayer-Schönberger', in D. DÉCHENAUD (dir.), *Le droit à l'oubli numérique,* Larcier, 2015, p. 328.

Certainly, the internet network relies primarily on a physical infrastructure. There is no internet without datacenters, submarine cables, terrestrial fibre optic, hard drives or microprocessors. Because information flows in binary language, it relies on electric signals, and, for so, on exchanges between powered on devices.
However, the internet sets also itself apart by its intrinsically international character that exposes it to a geographically multilateral diversity of threats. Whereas in most situations giving birth to a legal dispute, the international character is just an ancillary parameter making its resolution more complicated, this international character is quite systematic when the conflict is related to digital technology, because the structure of the Internet itself is fundamentally based on relations through computers and devices located in different areas of the planet. Internet is for sure the new realm of private international law.
Yet this international character opens the door to a behavioural observation of others, a large distance off, from a vantage point located on a territory where the law of the citizenship or the habitual residence is not relevant. Like the main character of Alfred Hitchcock's movie *Rear Window* (1958), who watched his neighbour's private life through binoculars, the digital technology makes distant and personal observation possible, even escaping from the application of the law of the country where the observer is located. This surveillance, based on data collection, analysis, market researches and strategical diagnosis, has turned the modern human being into a *Homo numericus* who is more seen, watched and scrutinised than ever before in history. Not only the States use this technology to monitor a huge mass of internet users – even, as Edward Snowden revealed[4], without publicly admitting it – but also the *Big Tech* do each second of every single day. An important part of the digital economy is based on collection and analysis of data.
This monitoring of the behaviour of others leads to a writing of a code line outlining the relevant traces the internet user has left behind him and summarizing his activities. Yet this code, which is not an analogue print but only a text, a *gramma* as would have said the Greeks[5], can be duplicated infinitely, circulating with ease. The collected data are not the physical trace of a step in the mud, the noise footprint on a magnetic tape, or the impression of light on a silver film, but only a *description by text* of what the person has done[6]. And it is very easy to circulate a text and reproduce it, whatever is its new medium, using electronic transmission channels. In other words, once the person has been watched, a fragment of what she has done is consigned to a text that can circulate from foreign

[4] E. SNOWDEN, *Permanent Record,* Pan Books, 2020.
[5] In Ancient Greek the word 'to gramma, atoς' litterally means letter, character or inscription.
[6] About the differences between the analogue print and the grammatic result of data collecting, see our study: 'L'approche Big Data en droit international privé', in A. FAVREAU (dir.), *La propriété intellectuelle en dehors de ses frontières,* Larcier, 2019, p. 200.

companies to foreign companies, from one country to another, without the person even knowing it.
It is well known that men need privacy and tend to live free from scrutiny. The idea is expressed in France throughout the famous expression of Sartre's theatre play *No Exit*, by which the main character, prisoner of the constant scrutiny of the others as deprived of privacy for ever, confess: "*Hell is the others*". But is also demonstrated empirically through the catastrophic experimental results of the prisons built according the *Panopticon* model drawn by the great British philosopher Jeremy Bentham. To Bentham, the ideal prison model had to be composed of cells set in circle, so that in the center a small crew of guards could enjoy a 360° vision of all inmates. Moreover, according this model, all detained could scrutiny themselves, from cell to cell, since all of these would be closed by a non-obstructing vision wrought iron gate. In other words, each prisoner could see, watch and scrutiny his comrades. This idea was based on a real privacy abolishment. Real experience showed it was the last thing to do. Prisoners of such a penitential center became mentally ill. Deprived of intimate space, they got sick and the *Panopticon* model was abandoned. Had we to learn from this terrible experience, we would say for sure that history has demonstrated privacy is fundamentally vital for human being. Being constantly watched is neither natural, neither positive.
In the digital era, the distant surveillance by data collecting has grown so much that the questions of visibility and *invisibility* has now to be seen in a completely different light. Since we have never been seen, even unwittingly, would it be legitimate to recognize a *Right to be invisible*? In order to answer this fascinating question, a proper definition of invisibility needs to be drawn (§ 1), before proceeding to all legal analysis it can lead to (§ 2).

§ 1 – What is Invisibility?

The invisibility has fostered myths, dreams and legends since the beginning of history. Reflections on this topic are not fundamentally new, except when it comes to the particular case of the digital invisibility in the modern age.

A) Invisibility in general

Before initiating a debate, it is essential to agree by convention on the specific point in discussion, so that its properties can be identified, without all misconceptions myths and legends can bring to mind.

1) Semantic specifications

The personal invisibility can be defined as the quality of a person whose existence, presence or action can not be perceived by others. If the person is invisible, no one can suspect her existence; or, at a

lower level, her presence at a specific place during a specific time; or, at an even lesser degree, what she is simply doing. The invisibility can have different grades, depending on the occultation power. But it bowls down to an eviction of the others perception power.

Thus, invisibility must be distinguished from other concepts.

First, it differs from *anonymity*. Invisibility is a genus of occultation which anonymity is a specie. A main characteristic of anonymity is to hide the true identity of the person. Anonymity is just a form of invisibility: the one of the name. The anonymous person does not necessarily hide her existence, neither her presence. One can be anonymous and ostensibly wear a mask; or, on the contrary, be anonymous by sending letters or releasing online a content without letting appear any geographical localisation. Anonymity, as the name invisibility, can be coordinated with other forms of invisibility or remain strictly limited.

Second, it differs from *invincibility*. The opposition may appear *prima facie* quite rhetorical. At first sight, the two words only have in common an alliteration. However, in our collective psyche, invisibility is an irresistible reminder of a sort of extraordinary power making its holder invincible and dangerous. In fact, nothing could be further from the truth. The simple reason for this is that magical invisibility does not exist. The only existing invisibility consists in the use of technical means to hide things or people from the others. But this concealment by physical tools can be dissipated by an opposite use of the same tools. Furthermore, from a legal and even ethical point of view, there should be no confusion between invisibility in itself and the potential misuses of it. For now, no rule requires the citizens to be constantly identifiable when they go out in the streets, by indicating conspicuously their personal identity. In a middle of a crowd, far from his habitual social environment, a man lost in a big city is already in a moderate invisibility situation. He is not at all "invincible". Nobody would seriously accuse him of planning a crime, only because his identity is perceivable at first glance. In other words, distinguishing invisibility and invincibility enlightens the fact that a certain form of personal invisibility is absolutely natural in human life, in countless situations, provided that this invisibility is reversible. Invisibility is not the tool of invincibility, despite popular legends. Remaining invisible, to a depending on circumstances extent, is not *per se* criminal.

Third, invisibility differs from *impunity*. If the invisibility does not necessarily lead to crime, it does not protect the invisible criminal by any form of impunity. Two reasons explain this. The first reason is that invisibility does not constitute any escape device on the ground of the law. Being invisible does not extract the person from the scope of application of the law. The second reason lies in the rebuttable character of invisibility technique. The "hex" dissipation is not only a technical question. It is first of all a matter of principle.

Not only the invisibility remains neutral *per se*, since it can be used properly in a virtuous manner, but it can even be the best evidence to demonstrate the *animus nocendi* of the person who used it in a dishonest way. After refraction, it can establish in Court the deliberateness of an action.

2) Invisibility properties

Invisibility distinguishes by four fundamental properties.
The first property is to be relative. Invisibility, as we may consider it in the real world, is limited in time, space and context.
It is relative in time as long as it requires the use of an artefact, which is quite always the case for a natural person. Whether it is about confining herself at home behind closed doors, windows and curtains, wearing face paint in the middle of a crowd, or acting discreetly, the very action of being invisible will always remain temporarily.
It is also relative in space, since anything or anybody can only be invisible from a certain point of view. Reality can be hidden to the human perception or the detection power of a machine, but only at a certain angle and for a specific kind of perception. This is the case, for example, of the person who hides the real meaning of her speech, and makes the authentical message invisible, when she uses a code. In this situation, the content of the communication is invisible for the non-holder of the code. But the communication itself is not hidden. In a similar way, the man who hides a knife in his pocket, for instance a mineral blade, will may be pass through the security checkpoint in an airport, without necessarily being detected. However, a body pat will easily reveal the weapon, despite its invisible character to the metal detector. In the same way, the cheater who deals the cards in a poker game and delivers himself a false hand, for instance a brilliant three of aces, can only reach the goal if he executes the move at the very moment when the other players do not watch him. Without this attention decrease – which professional cheaters designate by the word "*shade*" – cheating is impossible. As the famous Georges De La Tour's painting, *The Card Sharp with the Ace of Diamonds* (1635), gracefully demonstrates, cheating thrives on non-vigilance. Invisibility is never absolute: it remains limited to a perception angle, for an instant or during a limited period of time.
At last, invisibility is contextual. There is no absolute invisibility of persons or human matters[7]. In the City, the citizen's invisibility is always the result of a compromise or a turn of events. Obviously, it is still possible to define life by opposing it to death, as the famous physicist Xavier Bichat did when he said that "*Life consists*

[7] This paper is about the invisibility of a person, her possessions and actions in law. Its scope is limited to the social sphere. It is not on the natural, biological or physical phenomenon.

in the sum of the functions by which death is resisted"[8]. However, it is impossible to do the same if one tries to define the social invisibility, since there is no sharp break, definite and uncrossable between what is visible at a certain time and from a certain point of view, on one side, and what it is not at another time and from a different point of view. The truth lies in the *continuum* that links the visible to the invisible, depending on moments and circumstances. No absolute invisibility exists. One need only look to the opposite hypothesis. Consider an absolute and tight distinction between the visible and the invisible in the field of strictly visual perception. From this point of view, the opposites can be looked upon as the *shadow*, on one side, and as the *light*, on the other side. That being made cleat, what do we see in the *absolute shadow*? Obviously, nothing. However, what do also see in the *absolute light*? The answer is the same: obviously, nothing; since *in the absolute light, the eyes are dazzled*. No one can see anything in the total light, except a nebulous white texture that blinds. The conclusion that emerges from this is simple. Everything that is seen is only detected through a combination of *Light* and *Shadow*. The accuracy of this discernment, and for so of the perception of things and people, depends on a layout of the dark zones and the luminous zones, from a particular point of view in time and space. This layout is relative. It can only be defined regarding a figure, at a certain time, as the continuum of visible and invisible. In this sense, the absolute invisibility of the person and her actions simply does not exist in the City.

The second property of the invisibility lies in its rebuttable character. Each concealment method, or almost, can be rebutted. When it is no longer possible to reveal what has been hidden, it remains however possible to notice that something has been done to conceal specifically something. This rebuttable character may appear to be obvious, since all concealment is artificial. However, from a legal point of view, it must be underlined. The invisibility at a certain moment does not exclude an *ex post* identification of the person. Neither does it exclude the report of what she has done, so that she remains liable. Prohibiting the invisibility, in the name of surveillance efficiency and respect to the *imperium*, is mere misconception.

The third property of the invisibility comes from its moral neutrality. Contrary to what suggest popular beliefs, being invisible is neither good nor bad in itself. The hole thing depends on the use of this tool. Thus, the political opponent to a tyrant who uses invisibility techniques to hide his communications and get in contact the democratic press of a foreign country is not to be blamed. On the contrary, the drug trafficker who sales his illegal substances in a hidden manner commits a crime. In both cases,

[8] Ph. HUNEMAN, *Bichat : la vie et la mort*, PUF, 1998, p. 5.

invisibility is neither good neither bad. It is the vehicle for an action that one has to consider separately.
The fourth property of the invisibility emerges from its tactical ambivalence. As an advantage, from a martial point of view, it can be used defensively or offensively. To put in the mouth of the Common law, it can be used *as a shield or as a sword*[9]. Obviously, the offensive mode raises more reservations – except for law enforcement – than the defensive mode can do as a mere protection of privacy. The distinction must be highlighted, especially for legal developments.
Thus, it appears that the invisibility proceeds from an occasional character of a person or thing. It is not something completely unknown in any way. The literary imagination has captured the debate by absolutizing it on a binary base. Conceiving an absolute invisibility at a human scale from a legal perspective turns out to be a mere misconception. Such a bias would constitute the best way to jeopardize a fair analysis, letting popular beliefs on an unreal invisibility disturb the real justice. These beliefs are so lovely and deeply rooted in mind that their influence need not to be overlooked. Knowing them is for so the best way to keep them at bay, in the sea of myths.

3) Myths and History

From Ancient times to the present day, the invisibility has captured men's imagination. Let us get straight to the point: it has rarely enjoyed a good reputation, and its use has been regarded for the most as the symbol of evil, *hubris* and even assassination.
However, it is important to briefly browse through the mythological history it has given birth to, since the instinctive reactions its modern use can provoke in the digital world could be a result of this form of collective unconscious that determines – wrongfully according to us – a basically criminal comprehension of invisibility. Knowing the bias helps to nullify and see things in a more accurate way afterwards.
The most famous text on invisibility comes from Plato. In the Second book of *The Republic*, Plato expounds the recondite matter of *Gyges* from Lydia, an analphabetic shepherd who happened to find in a crevasse a mysterious corpse, which he immediately spoils, all decent apart. Among the relics, Gyges discovers a ring he removes from the dead's finger. As he wields it, he understands the

[9] In English law, the doctrine of waiver, also known as *promissory estoppel* allows the debtor required to pay the entire amount of his initial debt, whereas the creditor informally consented a partial debt waiver without any consideration, to plead his good faith in *Equity* and argue that the creditor breaches a promised word. However, this reprobation of a violation of his word by a gentleman word can only be accepted as a defence, not as a claim to ask for money. It is commonly accepted it can be used *as a shield and not as a sword*: *Combe vs/ Combe* (2015) 2 KB 2015. This distinction between the offensive and the defensive mode turns out to be particularly relevant, from an ethical point of view, in the matter of digital invisibility.

ring is magic. When the collet is turned outwards, the ring bearer becomes invisible. Gyges decides to use this power to commit crimes, then go at the King's court, where he finally kills him and rapes the Queen. Gyges becomes King himself, by crime and impunity. Plato tells the story through his brother Glauco's mouth, to explain how much it is difficult for a man to withstand the inclination of evil, when he has the power to escape from the guard, justice and humans in general. Justice is not innate in the individual, since it comes from the pressure the others put on him. As the invisibility suspends it, everyone, even the Just, would end up in committing crimes, if the Ring of Gyges was handed out to him.
Plato writes:

> "Suppose now that there were two such magic rings, and the just put on one of them and the unjust the other; no man can be imagined to be of such an iron nature that he would stand fast in justice. No man would keep his hands off what was not his own when he could safely take what he liked out of the market, or go into houses and lie with any one at his pleasure, or kill or release from prison whom he would, and in all respects be like a God among men.
> Then the actions of the just would be as the actions of the unjust; they would both come at last to the same point. And this we may truly affirm to be a great proof that a man is just, not willingly or because he thinks that justice is any good to him individually, but of necessity, for wherever anyone thinks that he can safely be unjust, there he is unjust"[10].

The discourse on justice appears to be the real topic of Plato's writing. It is about defining justice and object the idea of purely individual virtue free from any external constraints. But the invisibility, though used as pure metaphor, is precipitated into villainy. This bad reputation will be a curse for millennia.
The other most famous text on invisibility is obviously Herbert George Wells' novel, *The Invisible Man*[11]. Published in 1897, the novel tells the story of a genius scientist called *Griffin* – a pretty misanthropic man despised by his contemporaries – who succeeds in synthesizing a chemical substance that makes the person, if absorbed, completely invisible. Having tested it on a cat, Griffin decides to experiment himself the beverage. Become invisible, without any possible come back to his natural state, he starts as Gyges to lift his moral inhibitions. He begins his career by stealing, before threshing the people who had not considered him very well. Forced to cover his entire body and face as a serious burn victim would do, in order to socially interact without revealing his intimate secret, he makes people feel uneasy. This uneasiness sharpens his

[10] PLATON, *The Republic,* Book II, 360a, translation by Benjamin Jowett, in *The Republic,* Cosimo, 2008 p. 33.
[11] H. G. WELLS, *The Invisible Man,* First published 1897, Create Space Publishing 2018.

misanthropy and heightens his inclination to evil. He starts to plan the assassination of one of his previous collaborators, and even to crown himself as the King "*Invisible First"*, considering his state is now outside the Queen's authority. His unlimited madness leads him to negligence, and the inhabitants of the village where the assassination plan is supposed to executed finally succeed in grabbing and stoning him. Once he's dead, his lifeless body becomes visible again; while his notebook, containing the beverage formula, is retrieved by Marvel, a previous stooge of him who has bought an inn with the money they stole when Griffin was invisible. Ironically, Marvell is incapable of reading it, since the notes are incomplete and written in Latin, Greek and mathematical language, definitely secretive to the limited of mind of their new holder.

Again, Wells clearly describes the moral breakdown the invisibility can lead to in one's mind, as well as the terrible power it gives the user, before a tragical end in corruption, consumption and madness. As Plato, Wells conceives it through a criminal, addictive and corrupting perspective. He adds however an authentic legal dimension. The character's delirium, extending to crowning himself as a King of a "*Reign of Terror*", no longer being one of Her Majesty's subject, gives him the opportunity to raise the question about the authority of norms when the subject deletes himself[12]. For sure, it is pure speculation and myth. Every invisibility is rebuttable. The real problem is not the invisibility itself, but the irrebuttable character it has in the story. In fact, Wells investigates implicitly the question of the question of refraction: as long as the invisibility is rebuttable, Griffin remains a subject of law. He is responsible for his acts, once turned back visible. On the contrary, where refraction is no longer possible, invisibility becomes a path to crimes, isolation and madness. In the end, the illustrious writer reveals what could be identified as *the paradox of invisibility*; namely the fact that, contrary to common sense, an invisible person, if she does not betray her identity, attracts more attention than an ordinary person when she does something, because her action seems very weird, without author nor origin. When Griffin picks up a cup of tea, the scene before the other persons eyes is frightening for a normal person ; the cup is levitating in the air then inclined on its own. That is the reason why Well's character has to fully cover his body; if he uses his power to become rich, by stealing and killing, he still needs to live in the human community and, for so, to be seen. This *paradox of invisibility* is particularly relevant

[12] As Hart has brilliantly demonstrated that one of the characters of the legal norm lies in its persistence through time, albeit the physical death of the person who enacted it, whom he called *Rex*: H.L.A. HART, *The Concept of Law,* OUP, 1961, p. 61. It appears the topic of invisibility also raises the question of the norm's persistence *outside the field of view* of Rex. We incline to think this persistence is certain, due to a simple reason: every state of invisibility is temporarily and will necessarily be refracted. As invisibility is not impunity, the norm does not lose any authority, and still applies to the subject and what he furtively does.

today, in the digital age. The more an individual deletes all traces left behind him, the more he attracts attention in a paradoxical way, since he starts to act as a suspect, and not as an average man ignoring the discretion tools the digital technology can provide. In this respect, Wells' work provides a relevant reading in the modern era of invisibility.

At last, Tolkien's works provides the most mythical, philosophical and tragic vision of invisibility. In his masterwork, *The Lord of the Rings*, published in 1954, the Oxford's Professor describes a world threaten by the evil force of a powerful demon, Sauron. Sauron's power is embodied in the fancy world, the *Middle Earth*, in a doomed ring, which one of the properties it to make its holder invisible. This power arouses the excruciating envy and corrupts the soul of anyone possessing it. In order to save the Middle Earth, the only thing to do is to destroy the ring, which will require an entire war to protect it from men's madness, always subject to envy and power. Only then, once the ring has been finally destroyed, Sauron, who has remained invisible the entire war long, is definitely banned.

Even though the invisibility is not the exclusive theme of Tolkien's saga – unlike Well's novel – it certainly holds a central place in the description of Evil and the terrible power it can use. Again, it becomes the symbol of crime, horror and threat to the world. The tremendous success of the *Lord of the Rings* continues after Plato and Wells to anchor the idea that *invisibility is fundamentally evil.*

Beyond philosophy and literature, the idea of invisibility can also be found in a specific field where, this time, it is regarded as the pinnacle: the art of war. In this field, invisibility is the best weapon. Even though men have never reached a state of absolute invisibility, which only exists in fantasy worlds, the search for discretion and partial invisibility of the person and her actions occupies a central position. The most known example, in Ancient times, is that of the *Sicarii*. These zealot assassins stealthily murdered Roman officers with a dagger, before vanishing in the crowd, during the 1st century after JC. These inventors of what is today usually called *furtive murder*[13] based their strategy on terror, trying to destabilise the Roman authority in Palestine by striking unexpected targets and disappearing immediately after. Later, during the 11th century, the *Order of Assassins*, a Nizari Islamic group, will also use the same strategy to fight the Abbasid Caliphate and the Crusaders as well[14]. The art of assassination, joined to espionage, will also be cultivated in Japan, between the 15th and the 17th century[15]. More generally, the art of discretion has remained in

[13] R. D. LAW (ed), *The Routledge History of Terrorism,* Routledge, 2015, p. 18.
[14] B. LEWIS, *The Assassins, A Radical Sect in Islam,* Weidenfeld & Nicolson History, 2003.
[15] See the work of the founder of modern *Hoplology* – literally the « scientific study of weapons » - and specialist of Japanese ancient martial arts: D. F. DRAEGER, *The Art of Invisibility,* Lotus Press, 1977.

history one of the best weapons for States, and their special services.
The matter here is not about researching the history of invisibility in philosophy, literature and martial arts, exclusive of any legal perspective. Excellent works have been made, especially in the field of literature and social science[16]. The purpose of our approach is simply to explain why, culturally, the first reaction to the very idea of invisibility is pure hostility. Our common mythical, philosophical and literary background determines our reaction towards this kind of power. However, in the digital age, the situation could entirely change.

B) Digital invisibility in particular

Understanding the digital invisibility requires a prior examination of the framework in which it operates. The cyberspace does not have the same properties as those the physical space, since it opens the path to a mass surveillance no human society in history has ever known. That is precisely the reason why invisibility techniques have been developed, which can be used or misused depending on the person's intention.

1) Cyberspace properties

The cyberspace can be defined as the set of all information exchanges proceeded by digital tools and transferred from machine to machine. On this ground, it embraces the information exchanges proceeded on the Internet, which constitutes the most important part of it.
From this point of view, the cyberspace can be divided in several layers which reunion determines the functioning.
The firs layer is the physical one. It is made of input and output devices, datacenters, and pieces of equipment ensuring the connection and transmission under digital format, as land or sea cables, optical repeater, antennas, wave transmitters, etc. This infrastructure, that is strategically crucial nowadays, is the *sine qua non* condition to a proper functioning of cyberspace. An attack on one single component can paralyse an operator, while an attack on a major component, as a cable or datacenter, can compromise the security of the entire system.
The second layer is the digital one. From a physical point of view, the information flows through cables under the form of an electric or light signal. Antennas and wave transmitters propagate waves. But the emission and circulation are done through only two signals, positive or negative, depending on whether there is an emission or a lack of emission at a specific moment. Starting from this alternance, a binary language is used to code a message initially expressed through a natural human language, by assigning to each

[16] E. BARENDT, *Anonymous Speech : Literature, Law and Politics*, Hart Publishing, 2016.

combination of 0 or 1 an alphabetical or mathematical significance. The digital layer does not emerge from the emission of a signal in itself, which is only a physical phenomenon, in this case electricity or light. It comes from the interpretation that humans do by convention. *In other words, digital information is fundamentally a linguistic phenomenon*. It is a formed language, despite its vector, which is no longer the pharynx, nor the pen, but essentially electricity and light. This specification is important, not only for the understanding of the cyberspace as a structure in general, but also for a legal understanding. Because the digital exchanges are linguistic, plenty of questions that arise from them have to be firstly considered through a linguistic ground. The law of the language – that usually defines its legal status, the freedom of expression and the liability therein, the lawfulness of cryptography and secrecy techniques, the extend of the State's control on tongue, the meaning of legal expressions, etc. – is the key of any legal comprehension of digital information issues.

The third layer is economic. The cyberspace has given birth to worldwide economy. This can be distinguished in two. The first part is attached to the real economy. The cyberspace has here a function of pure communication between the economic operator. Instead of discussing, treating, offering, accepting and executing their agreements by postal mail, telephone or physical dialogue, the operators use computers. The execution of the contract can be simplified, since the linguistic instructions circulate through a faster vector. The second part of the digital economy arises from the functioning of the cyberspace itself. Here, two subgroups can be identified. One is about the economy of the cyberspace itself, so to say the wealth produced by the maintenance and development of the physical layer. Another subgroup refers to the autonomous economy produced through assets which value exist only in the cyberspace. Cryptocurrencies are the best example of this autonomous cybereconomy.

Under this presentation the properties of the cyberspace, as related to the question of invisibility, are double. Memory and surveillance characterize it.

a) Memory

The digital technology has its own memory. Unlike humans, machines do not think. They execute. The traces of all instructions and executions do not constitute an intimate journal of cognitive impressions, but a cold logbook without any sentiment nor personal feeling.

Why this precision? Because the human memory is based on *selection*. The oblivion function is vital to the balance of the psyche. The biological memory, contrary to what we usually incline to think, hinges on the deletion of what is irrelevant and the

conservation of a subjective print of what appears to be relevant[17]. From this print, later on, an image could be *reconstructed* to supply the contemporary needs of the person, in the particular context surrounding her. However, and strictly speaking, the human memory does not record the raw data of everyday life. Its function is to select. When this function is damaged and does not work perfectly anymore, the person can eventually suffer from a *hypermnesia*, which, far from being an advantage in society, will harm her personal life. The hypermnesia, that is to say the impossibility for the subject to forget irrelevant facts of his past, is unfortunately a pathology and not at all a happy skill.

On the contrary, the digital memory records unaltered signals, without any selection of subjective loss. The machine maintains a log of its activity, written in digital language, as long as an instruction to delete has not been given. Here lies a fundamental difference between digital memory and human memory as it is required in society. The human memory is supposed to focus on relevant facts and to delete irrelevant facts. It is also capable of recontextualising ancient facts when remembered in the present time. Machines record everything indiscriminately, allowing a consultation and analysis of the digital past without recontextualising it in the present. This property of the digital memory entails a tremendous capacity of surveillance. As soon as the machines are connected with one another, and if it is possible from one machine to another to consult the journal of its counterpart, everything that has been done inside a computer can potentially be known outside by a third party. The connection through cyberspace of plenty of machines allows a potential consultation, subject to the limitations of the law, of an accurate and descriptive memory which is completely disconnected from the present context. Obviously, the digital memory has tremendous advantages, for science and law notably. But as regards privacy, the digital memory is far more dangerous for people than the biological memory can be, since it allows a mass surveillance.

b) Surveillance

As soon as we consider the question of a right to be invisible in the digital space, we must underline the fact the cyberspace exposes all users to an entirely new form of surveillance history has never known. It allows a collection and analysis of data at a huge scale, which later determine or influence a various kind of political and economic decisions.

[17] *See* V. MAYER-SCHÖNBERGER, *Delete : The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2011, p. 16.

From this angle, the digital surveillance can be defined as the access to all or part of data and metadata of a connected device user, in order to analyse them for decision making[18].
Thus, it consists of not only data and metadata collection from a user of a connected device who consents to it in exchange of a free consultation of websites by private companies for marketing analysis, but also the same operation by States to observe how citizens behave. Both types of surveillance, under this perspective, have different goals and arises for so different questions as regards their lawfulness and legitimacy. As regards the private surveillance, the fundamental question lies in the reality of the user's consent who, as passive as he could be, does not generally know nor understand the extent and the importance of the data and metadata collected. It is also this of the economic model the web has generated. The free access to free services is in fact *paid by consenting to data collection*, so that data has become an exchange value. As regards the public surveillance, it raises the issue of the protection of citizens against the State, since the latter can now hold a new form of power that has never existed before. The intelligence services have always been existed, and it is normal for the Prince to ask them for an accurate description of what happens in the realm. However, this observation of the country can now be done at an entirely new level. In dark periods of history, no tyrant has never been in the position of knowing exactly what people think, do and plan, even at an individual scale. Today, it could be theoretically possible if such a tool fell in the wrong hands. The possibilities of repression and persecution of the population and minorities would be terrifying. For this reason, the question of invisibility is not only a debate about the protection of the person, as considered in herself. It is also a fundamental debate on the preservation of the rule of law.
Anyway, regardless of the goals, the surveillance is a fundamental state of the cyberspace in its contemporary form. Whether by *cookies, Java Script, Ghost Trackers* or *email scanning*, all neophyte cyberactivity is transparent. The slightest use of a connected too gives rise to a data or metadata collection; especially in the legal framework, since as long as the user consents, as the *General Regulation on Personal Data* (*hereinafter "GDPR")* provides in the European Union[19]. Besides that, the discreet surveillance by the States also exist, at different levels, depending on the political regime and the technology they have. The American *National*

[18] For the most, surveillance has economic and political functions. However, the personal surveillance also exists, if meant by this the fact for a natural person to observe through a digital tool what another person does, for a personal motive. This is similar to a detective work – if not spying when done illegally – and does not fall under the scope of this paper on the hypothetical recognition of a right to be invisible.
[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation), OJ 2016 L 119/1.

Security Agency's PRISM program revealed by Edward Snowden is a perfect example of the tremendous power and abuse this technology can lead to. According to M. Snowden, the NSA would have performed a potential monitoring of citizens, included foreigners in foreign countries by hacking the worldwide communication network. It is difficult to find a better argument in favour of a *Right to be invisible* from this perspective. Such a right, from this point of view, would be a form of legitimate defence.
Moreover, the surveillance can potentially be exercised outside the scope of the national laws. When it comes to analysing the data, the GDPR strictly rules the kind of analysis that can be conducted from the personal data related to the behaviour of people in the European Union. Thus, all data processing revealing ethnic or racial origins, political opinions, religion, health, sexual orientation and biometrics signatures allowing personal identification are strictly prohibited. Article 9 of the regulation is firm in this matter. There are exceptions, especially as regards such processing conducted to serve a public interest, protect people, or when the person has consented to such a processing in a special and explicit manner. But the question now being asked, as long one keeps in mind the intrinsically international and decentralized character of the internet network, is the efficiency of the European prohibition. When the data collected in the European Union – or from outside the EU by remote monitoring – are transferred towards a third State which is not bound by the GDPR or which escapes wittingly from its application, nothing stands anymore against the data processing despite their prohibition in the EU, before the targeted and incentive use of the results analysis in the European territory. As regards the US, the recently adopted *Privacy Shield* program guarantees control of the American Federal State on transfer and processing of all personal data collected within the European Union. The program is designed to guarantee an equivalent data protection in the US, as compared to what the GDPR provides. However, this program is legally contested before European jurisdictions, and some people suspected it of being mere alibi for discreet and free processing of European's personal data, as the previous *Safe Harbour* program was already regarded, before its expiration due to the *Strems's* decision (2015) of the European Court of justice. For now, the conclusion comes easily : it is not possible to assure the European citizens that their personal data will not be looked upon, once transferred outside the EU, for a data processing conducted in a third State which content and purpose would have been illegal in a Member State of the Union. From this perspective, there is no perfect cure against the surveillance in cyberspace, since what is legally regulated in a State can be free in another, where it is easy to transfer the data in order to escape from the law of the country of origin. The cyberspace is composed of a marquetery of laws where legal shopping is facilitated by the technical possibility of remotely acting, without

any physical move. At that level, it appears that transparency of people's life has never been so great in history and so powerful in its economic and political consequences. Yet, if this extreme transparency also produces perverse effects, there could be a cure, consisting in its perfect opposite: the *invisibility*. Proper techniques do already exist.

2) Invisibility tools

If we define invisibility as the occultation of a state, at a specific moment from a specific angle, as previously exposed, the search for this state is not Utopian ideal. Techniques exist. The present paper will only expound some, selected from the most commonly known according the operating process.

The first tool is the *Virtual Private Network* (VPN). It can be defined as a system that remotely creates a direct link between computers and isolates the information exchanges from the rest of the traffic on the public communication networks. Using such a tool, two users can have a remote conversation through the internet network without passing through middlemen, and notably without the access provider being able to consult data. All communications ordinary flow through the access provider. The latter constitutes a middleman who detains subsequently his customers data and metadata. The VPN creates, despite the intricacy of exchanges conducted on internet, a local network which only agreed users will have access to. It can be doubled, for security reasons, by a cryptographic system, in order to make exchanges impenetrable to any attacker who would succeed in intercepting them. It opacifies the content, and even more if cryptography is used, and artificially creates a local network for data exchange. Its purpose is to make the content and signification of communications invisible. It can hide the user's position and identity, letting him appear behind an apparent IP address. To enhance the protection, a VPN without any activity log can be used. At the moment a normal VPN is used, the access provider does not have information anymore on the computer activity. The operator providing a VPN service centralises the information, which channels only through him. Theoretically, the service provider could collect himself data and metadata of his customers. As regards metadata, he could record incoming or outcoming IP addresses, timestamp all connections, and measure the weight of the exchanges. As regards data, he could enlist the visited websites, the downloaded files as well as the used software. In other words, the surveillance is transferred from the access provider's hands to the VPN service provider ones. If the latter is located within the EU, he is submitted to the law of the State of his establishment, which can urge him to communicate to an administrative or judicial authority data and metadata of a

specific customer, especially if a public interest is threatened[20]. A *No Log VPN* is specifically designed to escape from such a possibility. It stands out due to the voluntary absence of any kind of activity log and its establishment and location outside the EU and the US, in order to escape from the competence and application of European or American law. Whether or not such a service provider can be trusted depends on the personal belief of the user, who can decide to rely on his professional reputation that can be documented by independent controllers. As it is often the case in the digital world, a corporate trust replaces the States control. With such a tool, on can remotely communicate without letting the access provider record anything, making the content of the dialogue invisible for him. This is a form of partial invisibility of the speech by exclusion of the ordinary intermediate.

The second tool that comes to mind is the *Tor* network. *Tor* can be defined as an alternate network superimposed on the Internet, which structure guarantees the users anonymity, on one hand, and the access to dedicate servers on the other. Initially conceived by the American army to ensure discretion of military communications, *Tor* is now for all available, without being at the same time too difficult for a basic user to manage. Through it, it becomes possible for the user of the dedicate browser, the *Tor Browser*, provided that he also uses a VPN, to watch ordinary websites without revealing his identity. The user can also get access to the deep web, that is to say to sites addressed in *.onion*, that remain unavailable without this technology. These sites make easy to consult, release or exchange information at an excellent level of anonymity, since it is technically difficult, if not impossible, to identify people hidden through the 'false' IP addresses provided by the browser. Using this creates a discussion lounge where invisibility of identity and location is the common rule. The use of cryptocurrency, to hinder all tracking by avoiding the classical banking network, completes the system by opening the path to financial untraceable transactions. This has allowed Tor to host a dark side, so called *Dark Net*, where illegal sites selling drugs, weapons, false IDs, counterfeit goods, or providing services such as illegal porn, that is to say composed of rape, torture or paedophile videos. It is difficult to quantify accurately the importance of this dark side of the realm of invisibility. Estimations have been made, however. According to a work completed in 2016 on a panel of 5205 sites, 1547 among them effectively provided illegal goods or services[21]. To generalize the estimation, the *Deep Web* will be composed of up to 30% of illegal sites. Obviously, it is huge. The proportion is probably much higher than the average criminal rate of the classical web. However, the discretion Tor provides also allows political opponents in dictatorial regimes to

[20] See for instance in France Article L 34-1 of the *Postal and Electronic Communications Code*.
[21] D. MOORE, T. RID, "Cryptopolitik and the Darknet", *Survival*, 2016, 58:1, 7-38, DOI: 10.1080/00396338.2016.1142085.

communicate freely and tell the democratic press what is going on in their country. It also helps journalists to get in touch with their sources without compromising them[22], and more generally enables each citizen to explore a territory where a perfect freedom of expression is guaranteed, since no control can limit it. Tor is both a democratic guard, a tool of freedom, and a perfect ally to commit crimes throughout the borders.

A third invisibility tool in the digital world can be identified in the alternative information networks that, despite their technical differences, also allows users to exchange information in discreet ways. The *Freenet, I2P* or *Zeronet* networks are perfect examples. *Freenet* is an anonymous network allowing consultation, email service and storage of encrypted information. *I2P* guarantees the anonymity by a using cryptographic key instead of a classical IP address, in order to make impossible any identification during the decryption process. *Zeronet* is composed of a peer to peer network in which data is stored encrypted by the users themselves, who can directly exchange using the platform that puts them in contact – as a broker would do – without relying on intermediaries who would potentially store data. Used through the Tor Browser, *Zeronet* allows to stay invisible and avoid censorship, provided it is used with caution.

A fourth invisibility tool, as regards the physical layer, is the *Tails* operative system. Normally, a computer keeps tracks of has been done on the hard drive. In other words, it could be compared to a ship, where the Captain keeps an everyday logbook. The physical seizure of the computer, once the hard drive has been extracted, makes a complete scan of the user's past activity possible. The search of a total invisibility leads to the complete deletion of all traces and memory of the computer, wich is exactly what Tails is designed for. Thought to work in read-only memory, without any information persistence once the computer has been shut off, it does not leave traces. Once the device is powered off, everything disappears. Even if the computer is physically captured, its analysis would turn out to be vain.

Last, but not least, the use of cryptocurrency is also a proper tool to be partially invisible online. As a unit of value agreed by convention by the users for their mutual exchanges, recorded in a log and protecting by cryptography their identity, the cryptocurrencies are a precious instrument of anonymous exchanges between individuals willing to avoid the classical banking network with its prudential control and regulation. The *Monero* currency, for instance, is a form of cryptocurrency particularly protective of invisibility, since its structure is made on purpose to prevent tracking of the payment originator, the transaction amount and the destination of funds. It becomes

[22] K. D. WATSON, 'The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks', [2012] 11 *Washington University Global Studies Law Review*, 718.

possible to "pay" without any third party to know who pays nor how much.
The use of these techniques allows the advanced user to watch, exchange and release information in avoidance of all personal identification and surveillance. Once invisible, the user can escape from censorship in a non-democratic regime, inform the public of scandal, or simply protecting his privacy if he wants to enhance it. He can also use this technology to get access to illegal materials or commit crimes. All this prompts the question of whether a *Right to be invisible* should be recognized, or, on the contrary whether this state of invisibility should not be looked upon as a subject of law's prerogative.

§ 2 – SHOULD A RIGHT TO BE INVISIBLE IN THE DIGITAL WORLD BE RECOGNIZED ?

For now, invisibility has always been regarded as a myth, not as a state which use could be a personal prerogative. Instead, it has been observed through partial manifestations, as anonymity or IP address dissimulation.
Nothings stands against opening a debate on invisibility though the fundamental rights perspective. Such an approach deserves attention. Firstly, it may unify the debate on all digital discretion techniques. Depending on the conclusion that could emerged, the ancillary analysis of all discretion tools will be clarified. Secondly, a general understanding could also cover the future stealth tools; and we all know in this matter that technique quite often precedes the law. The more the debate is cast at a general level of theoretical abstraction, the more the solution will be able to cover a diversity of similar situations. Thirdly, the choice of a high level of abstraction also comes from the clarifications that could be provided by the coexistence of the other fundamental rights, which a right to be invisible could eventually disrupt.
Following this approach, the fundamental question can be formulated this way: *Since the citizen has never been so watched in history than today when he uses digital tools, should a right not to be seen be recognized in our modern society, under the form of a right to be invisible?*
In order to answer this question, a close look at the wording is required, before. Only then can an answer be properly suggested.

A) Examination of the problem

The fundamental debate emerges from a reaction to surveillance and the natural instinct that inclines to preserve privacy, especially when it is seriously attacked.
However, a natural suggestion does not always stand up to scrutiny. This is why an examination of all arguments in favour or against the recognition of a right to be invisible appears to be appropriate.

1) Arguments pro

According to us, four arguments effectively plead in favour of a recognition of a right to be invisible. None of them would stand against a regulation, control or limitation of such a right, would it be recognized.

As previously explained, and as it is now widely admitted, the *Homo Numericus* has sacrificed unwittingly his privacy, through his personal data, in exchange of a free and easy use of digital technology. Citizens have never been so watched in the entire history by corporate companies or public authorities. There is no point ensuring a classical protection of privacy in analogue life, as Article 8 of the European Convention of Human Rights and Article 7 of the Chart of Fundamental Rights of the European Union, if this protection shrinks away due its insufficient character in the modern digital age. Privacy, and even the protection of personal data, have been initially designed at a time when the information circulated through analogue channels, such as newspapers, cathodic television, postal mail, or radio frequencies. Furthermore, most of the reading tools of the information also relied on sound or visual interpretation of an analogue print of the original signals, such as the sound of an instrument or a voice, or the light reflected by a person, on a physical medium, like magnetic tapes or argentic pellicles. These reading tools were not connected to each other, nor linked to an access provider. They did not record anything, and no data collection was possible. Things are completely different today. More than 98% of the information circulates under digital format. The communication and information techniques that have given birth, as a reaction, to the classical privacy are no longer used, except in 2% maximum of the situations[23]. The ordinary privacy and personal data protection have been literally phagocyted by the digital technology. One could object this phagocytosis has occurred by virtue of people's everyday consent; so that there would be no real *intrusion* in private sphere. When the person agrees, there is no intrusion, exactly as there is no break-in if when a person is invited at home for dinner. But this is mere illusion. Only few people are really aware of what they agree on by clicking on the "*I consent*" button. Moreover, a social and professional undeniable pressure is put on people every day so that they use the digital tools. This can be easily demonstrated. No citizen would accept for instance in the real world to read the papers comfortably sat on a chair next to the chimney, at the end of the day and back home after work, while a dozen of people working for private companies would join him in the living room to observe him accurately as a laboratory rat; even if, in exchange, the newspapers would be free… However, it is exactly what happened in the digital world when the same citizen

[23] *Interview with Viktor Mayer-Schoënberger, op. cit.* n.3, p. 326.

reads, without any technical skill, the same free papers on the Internet, through the ghost programs hidden inside. If there is such a difference between the natural reaction in the real world and the absence of reaction in the digital world, it is because citizens simply do not understand what is going on.

The second argument pro lies in the equality of citizens. The equal treatment principle is an essential component of the democratic regime. It is provided by Article 1 of the *Universal Declaration of Human Rights* (1948), Article 14 of the European Convention of Human Rights, and Article 20 of the Charter of Fundamental Rights of the European Union. Yet the technological intrusion on people's privacy, due to their passive or ineffective consent, on one hand, and to the mass surveillance on the other, could divide the population in two categories. The first category would comprise the people who are not aware of surveillance and digital observation, that is to say the huge majority of the population. It would also comprise those who, despite their comprehension of the problem, are not sufficiently skilled to use discretion tools online and make them partly invisible. On the contrary, the second category, largely residual, would include experts, talented amateurs and hackers who are, by definition, in the perfect position to use discretion tools without making any mistakes, such as cryptography, alternate networks and amnesic operative systems. This division of the population would lead to a different protection of privacy and personal data, based on people's technical skills. Experts would be protected, while laymen would not. At that point, one could object this different treatment would only be a *de facto* inequality, not a legal inequality. However, we could retorque the gap between the two categories would be so large that it would completely devitalize the right to privacy. The purpose of law is to yield to each one his right, not to proclaim ideals that finally end up in pure illusion and delusion. From this point of view, the efficiency of the principle equality would be worth recognizing a fundamental right to be invisible, totally or partially, in the digital sphere. And in order to ensure this right's efficiency, States would have a positive obligation to make simple digital tools available for everyone.

The third argument pro emerges from the intrinsically innovating character of digital law. This argument is essentially replicative, since it dispels the obstacle which immediately comes to mind and underlines that such a right to be invisible has never existed in history. It also refutes the technical opposition of those who would inevitably reply object that a such a right would be in any case technically impossible or dangerous for the digital economy. From that angle, the reply is simple. If a right to be invisible has never been recognized, it is because the visibility has never been so high as it is today. Admitting such a right would be innovative, but the problem it would solve is also entirely new. Furthermore, recent history has shown that a right to be forgotten could be recognized,

though it had been regularly said such a right would be technically impossible to implement. The European Court of Justice has recognized the right to be forgotten in the *Google Spain*'s case (2014), before the GDRP explicitly introduced it in the European data privacy law, through its Article 17. Private companies have adjusted to it *volens nolens* and demonstrated there was no technical impossibility for real.
The fourth argument comes in refutation from the consequences a persistent refusal of any recognition of a right to be invisible would lead to in the digital world. Whereas closing doors and windows at home is natural, when we want to be invisible from outside, there would be no right to do the same in the digital world. The latter would be bound to become a huge *Panopticon*, vital for working and having and social life, where everyone would have to pay his share by accepting surveillance on every breath he takes. This curious perspective would easily demonstrate the existing invisibility in the physical world only have to be transposed in the digital world by the recognition of a dedicated fundamental right.
These arguments are serious, as we can see. However, they also can encounter a serious contradiction.

2) Arguments contra

The first obstacle to a recognition of a right to be invisible can be labelled as the *police argument*. Everybody knows that the social life requires a legitimate, organized and efficient authority to enforce the law, through coercion if necessary. If there is no freedom without law, neither can live an organized community without police. The form and means of the police vary in history. But it always remains vital. To put in the mouth of the German philosopher Max Weber, the State has the "*monopoly of legitimate violence*". From this perspective, recognizing a right to be invisible in the digital world – so to say a right to escape from surveillance – would be absurd. It would be like blindfolding the eyes of the police. Could we imagine a society where policemen would wear a band on the eyes in order to ensure they cannot see the people they are supposed to protect, control or arrest? It would be a perfect scenario for the Theatre of the Absurd. If surveillance is a problem, then the debate should be orientated towards its content and form. Everything can be discussed. But not the very existence of a surveillance, except from an anarchist point of view. The police are the normal extension of the public authority's *imperium*. It is inconceivable to recognize a general right to be invisible, since it would amputate a vital organ of the political society.
The second argument contra comes from *law's clarity*. Indeed, in a healthy legal system, either a situation is submitted to norms, either it is not. Thus, if we consider the state legal order, accusing wrongly someone of a specific disgrace in public is not permitted, and constitutes a defamation. On the contrary, at home and within a

private circle, nothing legally stands against giving free rein to any personal hostility. If morality can eventually be affected, the law will not. The difference between these two situations lies in the *perimeter* of the defamation's prohibition. The latter only consists of public speech, not private ones. As a consequence, either the situation falls within the scope of application of the norm, and then the rule has to be applied effectively; either it is not the case, and then the rule does not have to be applied at all. But there are no intermediate situations in which the norm is applicable, while the person can legally avoid its appliance. In other words, waters are clear or opaque. A good legislation should not accept *turbid waters*. If one follows this reasoning, then a right to be invisible cannot be recognized at all. Such a recognition would lead to define and maintain a real ocean of turbid waters. Selling drugs would be forbidden, while using technologies to do so discreetly would remain legal. In fact, there would be no paradox in that situation, but only absurdity.

The third argument contra infers from the *absence of hierarchy among the fundamental rights*.

From a general point of view, it is commonly accepted the right to life oversees all the other fundamental rights. The reason for this is both ethical and chronological. The moral cannot accept and legitimate a legal system which purpose is to kill people. The very goal of a political society is to preserve life. It is the prime directive of any democratic regime. Even coercion – including its lethal form, especially in war times – can only be used to defend the citizen's life and enforce the norms that have been conceived at this goal. Furthermore, from a chronological point of view, life precedes the law. Where there are no subjects, there is no law. This is why the right to life substantiates all the other fundamental freedoms[24].

However, apart from the right to life, one can seriously doubt a hierarchy among fundamental rights can exist[25]. In international law, the UN General Assembly resolution of 1977 proclaim the indivisibility of fundamental rights, and the Vienna Declaration of June 25th of 1993 reiterates this principle[26]. There certainly are principles, underlaid by human rights, that deserve a strict protection, given the seriousness of their eventual violation, such as prohibitions of torture, slavery or retroactivity of criminal law[27]. Apart from this strengthened principles, the majority's opinion

[24] Ch. QUEZEL-AMBRUNAZ, V. RIVOLLIER, « Une hiérarchie entre droits fondamentaux ? Le point de vue du droit civil », *Revue des droits et libertés fondamentaux (RDLF),* 2019 chron. n°45.

[25] K. TERAYA, "Emerging Hierarchy in International Human Rights and Beyond: From the Perspective of Non-derogable Rights", *European Journal of International Law (EJIL)*, 2001, vol. 12, p. 917.

[26] A. SANGIOVANNI, *Humanity Without Dignity: Moral Equality, Respect, and Human Rights,* Harvard University Press 2017, p. 235.

[27] L. HENNEBEL, « Typologies et hiérarchie(s) des droits de l'Homme », *Annuaire international de justice constitutionnelle*, 26, 2011. Constitutions et droit pénal - Hiérarchie(s) et droits fondamentaux. pp. 423-435.

considers there is no hierarchy between the fundamental rights[28], or, in a more subtle way, that is very difficult to make it explicit[29]. The very idea of such a hierarchy is not completely rejected by all in the academic literature. According to certain authors, rights could be classified depending on their efficiency in keeping the dominant class in its higher position, from a Marxist point of view[30]. For others, they could be distinguished on the base of the possibility or impossibility of a waiver[31]. In any case, such a hierarchy would be highly implicit[32], since no international nor national instrument refer to it. The European Court of Human Rights considers in the *Stec c. UK* (2005)[33] case that "*The Convention must also be read as a whole and interpreted in such a way as to promote internal consistency and harmony between its various provisions*". Apart from the right to life, the Court is reluctant to admit a hierarchy among fundamental rights[34].

If we follow this thesis, then neither the right to privacy neither the right to personal data protection must be regarded as superior to other rights. *Privacy is not the Queen of Rights.* Yet if a right to be invisible was recognized, everyone could use in its own interest to escape from surveillance, control and police. Some would exercise it to commit crimes, harm people and violate the law. From this point of view, the right to invisibility would become the instrument, in the name of Privacy, to weaken all the other fundamental rights. Privacy and personal data protection would become superior rights, or almost, dominating all freedoms. Yet it is exactly what the absence of hierarchy among fundamental rights is supposed to prevent. For this reason, such a right to invisibility ought not to be recognized.

At last, a fourth argument contra emerges from what could be called the *treatment at source principle*. When a problem occurs, the best thing to do is to treat its causes and manifestations, until they disappear. Waiting and letting it flourish is not wise. Proposing later a revolutionary solution that will completely change the legal

[28] M. AFROUKH, « Une hiérarchie entre droits fondamentaux ? Le point de vue du droit européen », *Revue des droits et libertés fondamentaux,* 2019, chro. 43 ; J. D. MONTGOMERY, 'Is there a hierarchy of human rights?', *Journal of Human Rights,* 2002, Vol. 1, n° 3, p. 373 ; E. KLEIN, "Establishing a Hierarchy of Human Rights: Ideal Solution or Fallacy?", *Israel Law Review,* 2008, Vol. 41, n° 3, p. 477 ; A. TAHVANAINEN, "Hierarchy of Norms in International and Human Rights Law", 24 *Nordisk Tidskriftor Menneskerettigheter*, 2006, p. 191.

[29] Th. MERON, *On a Hierarchy of International Human Rights*, American Journal of International Law, 1986, Vol. 80, n° 1, p. 1.

[30] C. BROCKETT, *A Hierarchy of Human Right*s, Annual Meeting of the American Political Science Association, New-York, ERIC, 1978.

[31] L-Ph. LAMPRON & E. BROUILLET, « Le principe de non-hiérarchie entre droits et libertés fondamentaux : l'inaccessible étoile ? », *Revue générale du droit*, 2011, 41 (1), pp. 93-141.

[32] F. SUAREZ-MULLER, "The Hierarchy of Human Rights and the Transcendental System of Right", *Human Rights Review*, 2019, vol. 20, pp. 47–66.

[33] *Stec vs*/ United Kingdom ECHR 2005, no 65731/01 & 65900/01, § 48.

[34] See the opinion of judge Ergül in *Sahin vs Turkey* ECHR 2018 no. 16538/17. Judge Ergül considers that the very idea a legal hierarchy among human rights should be excluded.

system's equilibrium is not a good idea. The art of law is primarily supposed to prevent conflicts, not to generate or multiply them. In law, as in medicine, prophylaxis is a virtue. As a consequence, if the surveillance generates problems, due to the fact that citizens have never been so watched in history, regulating it with great care, instead of creating a new right that could jeopardize all the others, would be a more appropriate way. It could solve the problem without unbalancing all the legal system[35].
Each of these two theses is based on relevant arguments that reveal different facets of the problem. The resolution of the problem will not emerge from the complete rejection of one of them, but instead from their coordination.

B) Suggested answer

In order to solve the conflict between the citizen's protection and the digital transparency and surveillance, invisibility should be looked upon a different way.
From our point of view, it appears that invisibility has to be considered as a *fact,* not as a right. When the invisible person acts in the digital sphere, leaving few or no traces of she does, her state of discretion should not emanate from a *per se* right to be invisible. It is only a personal state that has to be understood as a simple fact, submitted to the legal regime under which its access and use can be characterized. In other words, the invisibility is just a consequence of an already existing right, not an autonomous prerogative of the subject that would have to be considered in itself.
If we follow this analysis, the legal regime of the invisibility does not require any legal invention, and certainly not the recognition of a hypothetical specific right. The only thing to do is to identify the legal regime in the different foreseeable situations, by confronting the facts to the rules of law. In a certain way, the old Roman principle *Da mihi factum dabo tibi jus* is still relevant today, since it turns out to enlighten the legal regime of the digital invisibility.
In other words, *the invisibility is ruled by the applicable law to the pre-existing right that has given birth to it.* Thus, the digital discretion can result from the inviolability of the domicile, or the right to privacy, the right to ownership, the freedom of expression, the freedom of contract, the confidentiality of correspondence, the legal regime of cryptography, the professional secrecy or the rights of defence.
Each time a digital discretion tool is used, the legal framework under which it is used will determine which law is applicable in private international law, and as a consequence what is its content.

[35] Such an approach could be inspired on the ECHR's solution about the surveillance of the workers' communications by the employer, which has to be proportionate : *Barbulescu vs/ Rumania* ECHR 2017 no 61496/08, § 121. Submitting all data collection and analysis to the person's consent, on one hand, with a legitimate interest and proportion on the other, could be an appropriate solution.

Some examples can demonstrate the relevance of this analysis.
Let us consider, first of all, the case to the protection of home. In private international law, the inviolability of home is normally ruled by the law of country of its situation[36]. As a consequence, if a person wants to protect her data at home by making untraceable all activity of the connected devices located therein, the choice to remove from the eyes of the surveillance, in particular by prohibiting all automatic data exchanges between the machines – so called *M2M* exchanges – , will be ruled by the law of country where the domicile is located. This solution fills in the *lacunae* in data protection as regards M2M exchanges[37], at least for those happening at home. The same applies to the use of VPN at home, for purposes not related to a professional activity. This use stems from the law of location of the domicile, notwithstanding any existing internationally mandatory rules – that is to say *lois de police* in the sense of private international law – that could eventually interfere.
Having regard to the use for non-professional purpose to anonymous and temporarily digital message service, whether it is on the Internet, or on an alternate network, such as Zeronet for instance. This kind of tool falls within the secrecy of correspondence. The user does not employ a manuscript, nor a classical email service. It is his personal choice. But this choice is ruled by the law applicable to correspondence. In private international law, this law is related to protection of privacy, which is an element of the legal status of the person[38]. As a consequence, the law of the citizenship is normally applicable for in the private international law systems of the civil law States of continental Europe[39], whereas in the private international law systems of Common Law, the law of the domicile of the person is applicable[40].

---

[36] In private international law, the liability of the perpetrator of a home invasion does not fall under the scope of application of the Regulation (EU) 2007/864 of 17 June 2008 the on the conflicts of laws in the field of non-contractual liability, since the violations of privacy are explicitly excluded from its scope of application (art. 1.2g). Each Member State of the EU applies its own conflict of laws system to identify the applicable law. In this matter, there is a common trend in comparative law in favour of the application of the law of the country where the tort has occurred (*Lex loci delicti*), so as a matter of principle the law of the country where the domicile of the person is situated. However, since the home invasion is before all a misdemeanour, one also has to consider that the inviolability of home in itself, apart from any civil liability, is territorially mandatory, so that it could be ruled by the law of its location, whatever is the law that rules the legal status of the person.
[37] S. STORMS, P. VALCKE & E. KINDT, "Rage against the machine: Does machine-to-machine communication fall within the scope of the confidentiality principle?", *International Journal of Law and Information Technology Law*, 2019, p. 372.
[38] The solution would be different if the correspondence has a contractual character. In that case, its use by the parties and the penalty in case of a violation of the convention on this ground should normally be ruled, according to us, by the law that rules the contract.
[39] In French private international law, the legal status of the person is classically ruled by the law of the citizenship of the person, since the old and famous *Busqueta* (1814) case, unless a specific provision submits it to the law of the habitual residence of the person: A. DEVERS, *J-Cl Droit international*, V° *État des personnes : statut individuel*, n° 20.
[40] J. HILL, M. NI SHUILLEABHAIN, *Clarkson & Hill's conflict of laws*, Oxford University Press, 5th ed., 2016, p. 317.

The applicable law to the legal status will define the lawfulness of the decision of using such furtive devices. This, again, notwithstanding the eventual interference of *lois de police*, that are likely to exist[41]. If it is the case, such mandatory provisions will rule the case on territorial base. In France, for instance, the service offer of electronic communication is highly controlled. Offering such furtive communication services could possibly fall under the provisions of the *Postal and Electronic Communication Code*[42], which could be identified as *lois de police*, applicable for so as long as the operator is established in France *(Inlandsbeziehung*), which is not quite often the case. On the contrary, for the subject, the use of this technology is free on the French territory, as a Statute of June 21st of 2004 provides[43], with the exception of the cases in which the Government can extract the encrypted data to clear them[44], as well as the judicial authorities for the needs of an criminal procedure[45].

However, let us now consider the use of such technologies for the execution of a concluded contract, especially if the convention provides the mandatory use of an encrypted communication system between the parties. Considering that the law that rules the contract also applies to this particular aspect would be logical[46]. This, again, withstanding the possible application of the eventual mandatory rules of the country of the establishment of the parties, before and during the period in which they exchange data by using such an encrypted system. In French law, the technical scheme has to be used in accordance with the system of prior declaration all cryptography system service providers are submitted to, with an authorization to transfer if the system is supposed to be used in a foreign country[47].

From a different point of view, if an attorney and his customer communicate by using a digital discretion tool, it appears logical to consider this situation falls under the applicable to the procedure (*lex fori*), as a consequence of professional secrecy and rights to defence. The procedure has to be conform with all requirements of the right to a fair trial, as enacted by Article 6 of the European Convention of Human Rights and Article 47 of the Charter of Fundamental Rights of the European Union.

Last but not least, the use of a verbal, graphical or sound code, by people using a non-encrypted communication tool is different. In

41 As far as we know, there are no cases in French law on this particular point, at least for now.

42 For instance, according to Article L 33-1 of this code, the service provider who offers access to electronic communications means is submitted to the system of prior administrative declaration.

43 Article 30 of the *Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*

44 Article 38.

45 Article 230-1 of the French Criminal Procedure Code.

46 See for instance, about the use of a VPN for teleworking and the need for the employer, who discusses the working time of the employee who sues payment of overtime wages, to show the data connection: Court of cassation, Cass soc 27 January 2016, no 14.13697.

47 See on this particular point the French decree no 2007-663 of 2 May 2007.

this case, people communicate through a natural clear language, while using a contrivance, so that the real meaning of the conversation remains impenetrable to outsiders. The announcement of the allied landing in Normandy on London Radio is a perfect example of this technique, as it was done through a quotation of a now famous poem of Verlaine: "*The drawn out sobs of fall's violins soothe my heart with their monotonous languor*". This discretion method is quite often used in a civil environment, since it remains the easiest way to hide the content of a message. Such an exchange, coming from a personal choice of confidentiality, falls under the freedom of expression as it is recognized and ruled in the country where the exchange takes place[48].

This legal analysis can be reproduced and transposed to any form of digital invisibility, whether it is total or partial. The main thrust is simple. Mass surveillance seriously threatens our privacy as well as fundamental freedoms. The constant progress of digital discretion tools may address some of this concern, at an individual scale. Confidentiality can be protected, however, without having to recognize an autonomous right to be invisible. The use of these techniques falls under the legal regime of the existing norms and rights under which they are employed. This paradigm of analysis, not only valid in private international law when it comes to identify the applicable law, but also in internal law to determine the relevant rules of the law of the State that have to be applied, does not extend to approval nor caveat as regards the digital surveillance in itself, nor its perfect foe, invisibility. The debate is still open, consequently, on the need for a more appropriate protection of privacy and personal data against digital transparency and surveillance, whether it is private or public.

[48] In private international law, the freedom of expression principle is mostly regarded on the ground of conflicts of laws through its abusive or defamatory use. In the French system, the famous *Press Act* (1881) is considered in international situations as a *loi de police*, so as to say applicable to any dispute before a French Court, whatever is the competent law designated by the rule of conflict in general: Cass Civ (1) 19 October 2004, no 02-15680.