SURVEILLANCE AND TECHNOLOGICAL (R)EVOLUTION. IMPLICATIONS AND REPERCUSSIONS ON HUMAN RIGHTS.

Michela Michetti[1]

Abstract
The impact of new technologies has generated disruptive effects on classic forms of surveillance. The surveillance models typical of modernity have been accompanied by unprecedented and pervasive control systems which, using the most powerful digital and IT levers, exercise unlimited and imperceptible power. In the era of post-modernity and the Internet, a new culture of surveillance was born with the exponential multiplication of controllers accompanied by the not entirely (un)conscious participation of those controlled. Against the backdrop of a scenario dominated by large "electronic eyes" and invisible power structures, the tension, at times irreducible, emerges between surveillance and the protection of rights. Hence the need to reflect on whether and how to preserve the "good" dimension of surveillance and, if anything, to build, alongside the power of the new "supervisors", further spaces to guarantee rights and freedoms.

Keywords
Surveillance, Power, Technological revolution, Big Data, Dataveillance, Human Rights, Data Privacy.

Summary

[1] Associate Professor of Constitutional Law, Department of Law, University of Teramo – Italy.

1. PROLOGUE. SURVEILLANCE AND POWER

In common and specialist language, the word *surveillance* evokes a sinister meaning[2], since its use has always been accompanied by the idea of control and exercise of power. Even before its definitional notion and its semantic value – developed mainly in the extra-legal context – surveillance is, in fact, an activity as old as the history of humanity[3], conceptually linked to the exercise of established power and for this reason mainly perceived as a negative-repressive activity.

An example of this are the *censuses* dating back to the 15th century BC., the *accounts* of ancient civilizations and those of the Catholic Church to control the spread of heterodox opinions[4]. Thus, again the use of telescopes, clocks in the workplace or maps to locate people, as well as the use of the best-known, English *Domesday Book* of the 11th century (a *descriptio* of the various landholdings), which allowed William the Conqueror to consolidate his power through complete and total knowledge of data about property,

---

[2] See CLARKE 1988, 498: "Surveillance is one of the elements of tyranny. The word conjures up unpleasant visions of spies, repression of individuals, and suppression of ideas"; LYON 2020, 23, who speaks of the term "surveillance" as a thorny term.

[3] See FOUCAULT 2014 *passim*; LYON 1997, 41: "Surveillance is not a new phenomenon. Since the dawn of time, we have 'surveilled' others to check what they intend to do, to evaluate their progress, to organize them or to take care of them"; SURACE 2005, 1: "It is important to underline that surveillance is by no means an unprecedented phenomenon before the birth of the modern state. Data has always been collected, we have always tried to classify, count, and describe information relating to categories of people in an orderly manner. Historically, populations have used censuses to organize themselves, to give themselves an order that served for the management of the army and the division of property. Once the calculations were carried out and the names and ages of the subjects were recorded, the sovereigns could establish how many men were suitable for combat, or how much land belonged to a head of family. There has therefore always existed the need, a primary necessity, for social control, an instrument through which order can be guaranteed for any form of society".

[4] See FIORENTINI 2023, 441-442.

inheritance and people[5].With these primordial features, surveillance has imposed itself and inserted itself into any form of society, since census, collection, cataloguing, classifying, counting data and information has always been the proprio of the exercise of power since *he who knows has power*[6].

Etymologically, *surveillance* derives from the French word *surveiller*, literally *keeping watch over* something or someone, in order to obtain information, data or elements, predictive and useful for knowing trends, characteristics, opinions and behavior both individual and collective. And in the transition from pre-modern to modern and up to post-modern, the semantic value of the term has not changed its original vocation, continuing to refer to the sense of an activity that conforms and orders societies.

In a writing from the early Seventies, *James Rule* defines *surveillance* as the methodical and specific attention on subjects, populations and personal details systematically monitored, recorded, controlled, consulted and compared[7], thus reiterating the existence of the almost natural connection between knowledge and power. In fact, in literature – especially sociological – the juxtaposition between power and surveillance constitutes a sort of hendiadys which well reflects what was taken up by *David Lyon* and underlined by *Antony Giddens*, for whom "*surveillance should not be considered only as a sort of reflection of capitalism (control over factory workers) or of the nation-state (keeping administrative registers of citizens), but as a true generator of power*"[8].

In every era, as in every sphere, the relationship with power has constantly emerged, but it is certainly with the advent of the nation-state that surveillance has become the specificity of modernity[9].

---

[5] See LYON 1997, 42.

[6] SURACE 2005, 3: "The more complex the society, the more the acquisition and conservation of power is based on the central role of knowledge".

[7] See RULE 1974, *passim*; LYON 2020, 1997, *passim*.

[8] See GIDDENS 1990 and LYON 1997, 20.

[9] See CALENDA, FONIO 2009, 21, for whom the advent of modernity incorporated the ancient practices of surveillance and control into routine, making them become systematic,

From the military field to factories, from schools to hospitals, from state administration to capitalist enterprise, *surveillance* becomes *a strategy* (of power) or an integral and axial part of the process of acquiring and consolidating authority to the point of generating important changes also on the organization and construction of anthropic spaces. Not only does the institutional conception of the way in which power is exercised change, but for example the architectural[10] rules also change which, forced to review the usual design and construction techniques, begin to favour circular, open structures, made of passages and transparencies which, as *Foucault* states, they "expressed a certain political utopia" [11] and allowed a form of multiple, anonymous, and permanent control of workers, sick, condemned and schoolchildren.

Moreover, this will be the cultural *humus* on which the architectural figure of *Jeremy Bentham's Panopticon* will blossom, taken up and theorized later by *Foucault*, as an archetype of modern surveillance power, in which the apparent and unverifiable omnipresence of the inspector induces in the prisoner a conscious state of visibility that ensures the automatic and de-individualized functioning of power[12]. And if in *Weber*'s theorization control

indeed: "it could be said that modernity itself is partly defined by these processes of routinization and systematization".

[10] SURACE 2005, 2, she captures this aspect even in the pre-modern era: "In the city-state the prince/feudal lord is the absolute master. Architecture is functional to the maintenance of its privileges, among which there is that of knowing everything that happens within the city walls. The central square, in which market activities, liturgical events and social relations between subjects take place, is located in front of the sovereign's palace. Just look out to check everything. The eye is the sense of control par excellence. And where it cannot reach, where hearing is also needed, the task of surveillance is assigned to the militia that patrols the streets and alleys".

[11] See FOUCAULT 1975, 190.

[12] See FOUCAULT 1975, 219-220: "Therefore Bentham laid down the principle that power must be visible and unverifiable. Visible: the prisoner will continuously have before his eyes the tall outline of the central tower from where he is spied on. Unverifiable: the

is a precondition for an efficient organization, for *Foucault* surveillance is self-disciplining and, in any case, in both cases, power and knowledge are two sides of the same coin.

The panoptic model becomes a tool of great impact for the organization and exercise of authority which, extendable everywhere[13], "produces homogeneous effects of power", so that without resorting to means of force it brings "the condemned man back to good conduct, the madman to calm, the worker to work, the student to application, the sick to observance of the prescriptions"[14]. And it will be a model that will come true within the folds of the modern state, where the power of surveillance will reach its most complete expression with the birth of the *surveillance society*[15], which will override the model of the *disciplinary society*[16].

---

prisoner must never know if he is being watched in the current moment; but he must be sure that he can be continuously".

[13] See FOUCAULT 1975, 224: *Panopticon* "It is – subject to subsequent modifications – applicable to "all establishments in which, within the limits of a space that is not too large, it is necessary to keep a certain number of people under surveillance". In each of its applications, it allows us to perfect the exercise of power".

[14] See FOUCAULT 1975, 220-221.

[15] The expression was first coined by MARX 1985, 21-26: "(…) the computer are creating a society in which everyone, not just a few suspects, is a target for surveillance"; LYON 1997, 16: "The minute details of our private lives are collected, stored, fished out and processed daily within powerful computer databases belonging to large companies and state bodies. This is the 'surveillance society'"; TRAVERS 2022, 15.

[16] See DELEUZE 2000, 234 ss., and PERRI 2020, 9-10, who reports that "all the internment environments functional to Foucault's theories on the exercise of power (family, school, barracks, hospital, prison) had now gone into crisis and, therefore, were no longer suitable for explaining society"; DELEUZE 2000, 238: "The old sovereign societies operated simple machines: levers, pulleys, clocks; while recent disciplinary societies were equipped with energy machines, with the passive risk of entropy and the active danger of sabotage: control societies operate with machines of a third type, information machines and computers, whose passive danger is interference and the active one is piracy and the introduction of viruses".

A power that will change its skin following the birth of capitalism and its rationalizing demands which, by having a significant impact on the entire social structure, will favor the rise of new subjects to be included and represented in decision-making bodies[17]. With modernity, surveillance will in fact lend itself to an ambivalent reading: it keeps all its original negative-repressive and security dimension intact[18], but to this adds the integrative and complementary one, to the recognition of active citizenship[19].
According to *Alexis de Tocqueville*, in modern mass democracies, the collection of information allows us to respond to the demand for social participation[20] and, by eliminating the inequalities of insurgent capitalism, allows the rebalancing and redefinition of the conditions of civil and political freedom. Surveillance thus becomes instrumental in the exercise of citizenship rights according to the paradigm of modern democracies[21]

---

[17] See SURACE 2005, 7: "The rationalizing demands, made its own by capitalism, are part of a process that involves the whole of modern history. Every area of life is influenced by them. The formation of the Western state, in the form we know, is their fruit. This involves a great transformation: the mutation of the forms of power".
[18] See MICHETTI 2023, 445: "The security-surveillance relationship is almost resolved into an imperative equation which in the risk society, like the one we live in, tends to prevent possible deviant conduct. The need for security and, therefore, control has grown as society has become more complex, and was significantly reawakened after the terrorist attacks of 11 September 2001, which, by redefining the trajectories of global geopolitical relations, dramatically re-proposed that the priority of the political agenda of the States is the strengthening of surveillance systems".
[19] As LYON observes, 1997, 52: "It is important to note that this emerging 'surveillance society' has more than one face. It can be seen both from the perspective of social control, and from that of social participation. The administrative apparatus established during the nineteenth century can be interpreted as a negative phenomenon – Weber's 'iron cage' of bureaucratic rationality or Foucault's 'disciplinary society'– or, in a more positive sense, as a means of guaranteeing all citizens equal treatment".
[20] See TOCQUEVILLE 1992, 219.
[21] See LYON 1997, 54: "Modern surveillance is simultaneously a means of social control and a guarantee of social participation rights. Surveillance has two faces. The birth of the 'surveillance society', then, is inextricably linked with the growth of the modern nation-

which, by incorporating ancient control practices and systematizing them through a pervasive process of bureaucratization, welcomes post-Enlightenment egalitarian demands, develops antibodies towards an increasingly more urbanized and industrialized society, and recognizes the citizen with a set of rights of social and political participation[22].

From this perspective, *surveillance* presents itself as an aspect of modernity and democracy and is linked to them as an unavoidable extension of the need to govern and support the complexity of the new social-political-economic and institutional order. And if, on the one hand, it contributes to the organization and coordination of the state administrative machinery, as well as of the capitalist enterprise and the military army; on the other, it remains an unmistakable tool for obtaining power. *Surveillance* implies, at the same time, diffusion, multiplication and strengthening of (the forms of) power; forges the new *physics of power* and gives shape to a new *political anatomy* that develops within the continuous and almost structural relationship between surveillance and power, since as *Foucault* observed "the panoptic device is not simply a hinge, a gear between a mechanism and a function; it is a way of making power relations function within a function, and a function through these power relations"[23].

2. SURVEILLANCE AND POWER: THE EFFECTS OF THE TECHNOLOGICAL REVOLUTION AND THE NEW CULTURE OF SURVEILLANCE

state. As the range of requirements necessary for administration expanded, bureaucratic organization evolved as a means of coordinating the various activities (…)".

[22] SURACE 2005, 2-3: "Thanks to the information collected on citizens, the State learns who will be able to benefit from public assistance, who will have the right to vote, and, above all, by recording the data concerning every single member of society, it will have an important means of guaranteeing an equal treatment for everyone".

[23] See FOUCAULT 1975, 241 ss.

If it is true that *surveillance* has covered and innervated the history of humanity, paced social and institutional transformations, it is also true that such changes have ended up affecting and innovating the forms and systems of surveillance. It has always been that way. And nowadays, a similar transformative/adaptive process appears particularly evident under the shock wave of the imposing *technological revolution* which has given rise to new spaces and new powers, to the point of restoring an unprecedented geography of power and its borders[24] and, consequently, a different conception of surveillance.

As it is known, revolutions have always produced important and profound changes, redesigning the coordinates of geo-political relations, socio-economic relations and obviously legal-constitutional systems[25]. Of all the upheavals and transitions that have occurred, there is no doubt that the *technological* one is the most impressive of the *revolutions*[26]: it catapulted us into the so-called *Digital Age* and into that space, so-called *cyberspace*[27], virtual and interactive, characterized by the de-territorialization of legal relationships, freed from any territorial reference which, fluid and infinite like the sea[28],

---

[24] See MICHETTI 2021,114.

[25] Technological innovation represented the first and perhaps most powerful push towards the space revolution. See ORTINO 1999, 11 s.; MANGIAMELI 2020, 238: "the driving force of this transformation is given by the idea of the network which, with the contraction of the time-space dimension determines not only the overcoming of the national economy, but also that of the territorial authority par excellence, the State".

[26] SCHMITT 2005, 96, the Author here underlines that "every progress in human technology produces new spaces and unpredictable modifications of traditional spatial structures"; ID. 2006, 11; KISSINGER, 2020, 338 ss.: "Cyberspace (...) has colonized physical space (...)" and that the effects of this revolution extend to every level of human organization so much so that we can talk about cyberdomain.

[27] AMATO MANGIAMELI, 2023, 101: "Cyberspace is the interactive virtual environment generated by the computer (...) whose nature is communicative and non-territorial".

[28] SCHMITT 1996, 20: "the sea, on the other hand, does not know such an evident unity of space and law, of ordering and localization (...). The sea is free. This means, according to recent international law, that the sea does not constitute a state territory and that it must

ignores a time-before and a time-after; it knows only movement, acceleration and ubiquity and is devoid of borders, a center, a periphery and scalar hierarchies. There is no doubt, therefore, that the extraordinary impact caused by technological progress has exposed the traditional spaces of power (state/national), to a substantial redefinition, and generated unprecedented arenas of power that exploded under the blanket of an a-spatial and post-territorial *nomos*[29].

Since the 1960s, the technological innovations of telecommunications, electronic information and the globalized economy have imposed themselves, with pervasive force, onto every aspect of political, cultural and legal life, *bypassing* the borders and territoriality traditionally considered to be ordering elements of power *tout court*. As a result, distance has become closeness; the non-place place; the remote synchrony, and the unity of Political life has cracked in the close impact with the emerging headless and *footloose* global power systems, unanchored from defined and confined spaces.

The proliferation of these new digital private powers (Big Tech, Social media, Rating agencies, the Web) – which continually challenge public authority and compete with it on a daily basis, exercising a power that is only formally "private" but substantially "authoritative" in appearance properly publicistic[30] – has unleashed the power of *networking*[31] and

remain open to all equally (…)"; AMATO MANGIAMELI 2023, 101: "the absence of the territorial element means that there are surfers (net-surfers) and that only surfing, i.e., navigation without a specific destination, adapts to the needs of the network".

[29] See SCHMITT 2005, 96.

[30] See ESPOSITO 2003, 6: "subjects who act in the forms of private law but who, due to their particular position of economic and/or social strength, are capable (...) of carrying out substantially authoritative acts"; PARUZZO 2022, *passim*; MANETTI 2023, 15.

[31] See CASTELLS 2014, 365: "these technologies have unleashed the power of networking and decentralization, forces that have practically undermined the centralizing logic of single command and vertical and bureaucratic surveillance. Our societies are not orderly prisons, but disorderly jungles".

generated new types of *surveillance*[32]. From this new perspective, marked by the inexorable revenge of the machine on man, a new *culture of surveillance*[33] develops, which is different and, in some ways, far from the dystopian vision of *George Orwell* in '*1984'* [34] and from the panoptic one of *Foucault.*

Faced with similar scenarios, the State, which now appears as *one* of the many forms of organization of power, is destined to relocate itself within the global/digital continent. Its traditional functions are reconformed within more fluid trajectories, overcome and surmountable by the – almost uncontrollable – speed of electronic communications (Internet), the pressing circulation of capital, investments, people, goods, services, and information. So that even surveillance, as a function/power of the State, is reshaped and takes advantage of control techniques that come out of the typical container of modernity (government departments, workplaces, control agencies)[35]. It is no longer, or no longer only, surveillance of Foucaultian and panoptic inspiration[36]; the *way* of carrying out surveillance

[32] See DANDEKER 1990, 46.

[33] See STAPLES 1997; McGRATH 2004; FINN 2012.

[34]which "'however futuristic' and still very topical. Orwell's work is not adequate to explain the prevailing culture of contemporary surveillance, which takes place in everyday life, starting from the use of cell phones, smartphones, or the purchase of any object on the internet", as HELZEL 2023, 146.

[35] See LYON 1997, 59: "Administrative surveillance, which once took place primarily within the borders of the nation-state, now expands beyond the old territorial limits, most obviously in the form of international intelligence networks. (…) Likewise, when searching for data on consumers in the global market, commercial surveillance forgets about borders".

[36] PERRI 2020, 9 ss., who underlines the epochal transition from the "society of discipline" to the "society of control", believing that "The surveillance of the controlled, unlike that of the disciplined, proceeds through incessant and very small adjustments between the network and what is intercepted".

changes thanks to the use of new information technologies, resulting in a qualitative and quantitative transformation[37].

The surveillance of contemporaries marks the transition from "paper" to "electronic"[38] surveillance which becomes less visible and more insidious, "multifaceted, complicated, fluid and rather unpredictable" [39]. Hence the new culture of surveillance: it is no longer "solid and fixed" as in the past[40] but, in perfect harmony with *Bauman*'s liquid modernity[41], it is flexible, mobile and widespread, capable of inserting itself into every minute space of people's lives and not only[42].

Alongside its "qualitative mutation"[43], *surveillance* has changed quantitatively, multiplying on multiple and different levels. The a-spatial character of the Internet produces and reproduces countless *surveillances*, giving life to a sort of updated re-edition of the panoptic institutions. The so-called

---

[37] See HELZEL 2023, 147: "the transition from modernity to post-modernity has decreed a real 'qualitative mutation' of the same criteria that regulate surveillance practices, so much so that we can claim to be faced with a new 'philosophy' of surveillance"; NIGER 2008, 11.

[38] See LYON 1997, 67.

[39] See LYON 2020, 44 ss.

[40] See LYON 2020, 44 e 45: "While surveillance was once solid and fixed, it is now increasingly fluid, which in turn contributes to the liquefaction of everything from national borders to identities".

[41] To borrow an expression from BAUMAN, LYON 2013, VII: "the expression "liquid surveillance", rather than an exhaustive definition of surveillance, is above all an orientation, a way of contextualizing the developments of today's fluid and disturbing modernity. Surveillance tends to become liquid especially in the sphere of consumption. When fragments of personal data extracted for a specific purpose become easily usable for other purposes, the ancient points of reference disappear. Surveillance spreads in hitherto unthinkable ways, reacting to liquidity while helping to reproduce it"; HELZEL 2023, 148; LYON 2020, 45-46 ss.

[42] LYON 1997, 80, taking up the teaching of Gary T. Marx, he reports that the new surveillance "transcends distance, darkness, and physical barriers. It transcends time, and this can be seen above all in the data storage and retrieval potential of computers (…)".

[43] HELZEL 2023, 147.

Cyberpanoptic, acting in non-places or in non-physical spaces and "on bodies profoundly changed by immersion in the flow of electronic communications and which branches out and spreads everywhere"[44], makes surveillance unlimited and increasingly imperceptible. More public and private supervisors are crowded within these new spaces, they process data continuously and from every segment of society, extrapolating behavioral models and the information is "forcibly directed towards certain objectives" [45] and together with these also life (and, above all, the behavior) of those under surveillance is continuously observed and, even more so, automated, modified and channeled towards specific purposes[46].

Nowadays, surveillance society, as defined by *Gary T. Marx*, no longer rests on a single *Big Brother* but on many *Big Others* and on different forms of surveillance not confined within the panoptic disciplinary paradigm[47], but

---

[44] See RODOTÀ 2004, 164.

[45] See PERRI 2020, 17, referring to the services offered by Big Data: "which are able to predict our desires even before they manifest themselves thanks to the application of need-to-know techniques".

[46]This is what ZUBOFF 2019, 18, defines as "exploiting ideology" or the new conception of surveillance whose objective is to automate us and direct human behaviour towards new ends.

[47] AMATO MANGIAMELI 2000, 22: "unlike the metaphors of the Panopticon and Big Brother, whose referent is a central coercive power, everything now revolves around the fact that surveillance takes shape in special places, in IT non-places, where continuously introduced information becomes the contingent measure of all things, where automatically assembled data binds everyone and everything, where the results involuntarily change entities, meanings and lives on a global scale. In fact, if the border lines between inside and outside are problematic, if the center and the periphery are continuously and randomly reorganized, surveillance cannot help but become horizontal: so as to transform everyone (human and non-human actors) into potential overseers of something and of someone"; CURCIO 2022, 29: "In the digital continent, whose connection and institutional framework is decidedly hegemonized and equipped by organizational models and machines functional to the growth of digital capitalism, the panoptic paradigm, although still operating in specific closed subsystems or in total institutions inherited from the twentieth century, is always less so in the new territories of expansion characterized by clear

much more penetrating than through the new IT technologies (computers, drones, controls and biometric detections) evaluate, train, orient, select, exclude and monitor human conduct and people[48]. Controllers monitor everywhere[49]; in every sector of society there are countless eyes that watch and draw data of any type, generating a model of *Surveillant assemblage*[50] from which individuals can neither escape nor remain anonymous[51]. In fact, they are inside a large *electronic cage* that contains them all and classifies each of them[52].

2.1. NEW SURVEILLANCE AND DATAVEILLANCE: SOCIAL CONTROL THROUGH THE POWER OF "DATA"

The new *culture of surveillance* has redesigned the forms and methods of the activity of those who, for the most varied purposes, make control a formidable instrument of power. Whether for economic-commercial

---

discontinuity with the past. In other words, it has had its day, and today it is no longer able to conceptually equip the social analysis of new territories".

[48] See BAUMANN, LYON 2014, 47.

[49] CURCIO 2022, 30, who, taking up the words of *Didier Bigo*, states that "today there is no centralized version of the Panopticon and that the device, if it exists, is fragmented and heterogeneous".

[50] See PERRI 2020, 11, which takes up the reflection of Haggerty and Ericson to underline how today surveillance activities are "pervasive, widespread and responsive to different purposes, including those linked to economic and profit dynamics". In fact, "not only the State apparatus, but also the private ones, are interested in monitoring the population although driven by different objectives. (...) everyone is subject to a multitude of supervisors, who separate the individual into a set of flows of information, which flow into databases that are very easy to connect to each other".

[51] PERRI 2020, 13; CIPOLLONI 2023, *passim*.

[52] See LOSANO 1986, 14-15: "the development of information technology and telecommunications networks have now made society transparent. The citizen feels watched with no possibility of escape, like a goldfish in its glass bowl".

purposes, or for socio-political or even security rather than recreational-communicative purposes, we are subjected to continuous and inscrutable control which makes us *transparent* to large electronic eyes.

Certainly, the acceleration, but also the facilitation, that the evolution of information technology and telecommunication networks has given to surveillance activity is unparalleled. There is an element, in fact, that today's technology mocks: it is the physical space in which the supervisor-surveille relationship once took place, and mostly ended. But not only. It was not only the *space* of surveillance that has changed. If it is true, in fact, that virtual space has been added – if not replaced – to physical space (circumscribed, finite, confined,) as a substantially unlimited place to exercise control, it is equally true that, along with it, it has changed the (*s)object* of surveillance. And if the *body* has always been the privileged observation point of control activity[53], today the latter extends to everything that the materiality of a body brings *with it* and *beyond itself*. While continuing to be observed, scrutinized, and monitored from a more strictly anthropomorphic perspective, it becomes an extraordinary vector of data and information that allows for almost total and continuous control. Therefore, it is no longer the signature

[53] MARZANO 2004, 47: "a sort of reflection of the multiple pressures and transformations of society, a receptacle of the values and beliefs that predominate in this or that culture".

or the serial number that identifies the person[54], but an aggregate of data that emerges from his constant observation[55].

It is no longer the *body* in its immediate physicality that is relevant, but what it becomes in the impact with the *information society* which transforms its function and role. "The individual is replaced by a new type of social being, the *dividuo*, or an abstract aggregate of information" [56].

And the society of "*dividui*" and of "*dividuazione*" is the one which, for *Deleuze* and *Guattari,* has displaced *Foucault*'s disciplinary society. Today the *body* conveys blocks of fragmentary information and individuals are *profiles*

---

[54] See DELEUZE 2000, 237: "Disciplinary societies have two poles: the signature that indicates the individual, and the number or serial number that indicates his position in a mass. The point is that for the disciplines there is no incompatibility between the two poles, that power is at the same time massifying and individualizing, that is, it constitutes those on whom it is exercised as a body, and models the individuality of each member of the body (...). In control societies, vice versa, the essential thing is no longer a signature or a number, but a figure: the figure is a pass, while disciplinary societies are regulated by passwords (...). The numerical language of control is made up of digits that mark access to information or denial. We no longer have to deal with the mass-individual couple. Individuals have become "individual", and the masses of samples, data, markets or "banks""; PERRI 2020, 10.

[55] See Regulation UE 2016/679, art. 4 " 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"; CIPOLLONI 2023, 384: "profiling is a technique used mainly for commercial purposes. Data analysis, in fact, allows the data controller or data controller to acquire a considerable amount of information for the purpose of developing marketing strategies that are as personalized and calibrated to the preferences of the user or the category of consumers in which they have been included".

[56] See MUBI BRIGHENTI 2009, 39: "From this perspective, surveillance processes are no longer interested in observing people, but rather in tracing a series of movements (not only and not so much of individuals, but of money, choices, habits – in short of information), in a way that allows surveillance agencies to differentially regulate access and prohibition of access to specific spaces and specific services for specific subjects".

identified through data flows that include "both bodies and minds" [57]. Flows of personal data that computer *databases* collect and store and when crossed and placed in mutual relation return a specific electronic *profile* of the individual[58], which according to a given taxonomy will classify him as *deviant*, *dangerous*, *asocial*, *defaulting*, *progressive*, moderate etc. [59]

The classification society, through the systematic categorization of data, creates a *data-image* of the individual: a *virtual alter-ego*, not a body but an information system, a disunited, decomposed, and incorporeal form resulting from the combination of numbers[60], and this *Super-ego*, "(this) 'other individual' enjoys an existence separate from the real individual"[61]. The new surveillance techniques, as *Lyon* further states, tend to be based on abstractions rather than concrete people. The *data-image* is its product, being nothing more than an assembly of data obtained from the observation of individual or collective behaviours. The digital language of control is, therefore, a language of *figures,* and is fed by the accumulation and aggregation of data intended mostly for the needs of the new economic order.

---

[57] See BARANZONI, VIGNOLA 2015, 165.

[58] See CALENDA 2009, 67: the *Electronic profiling* is a technique that associates an individual with a group with similar characteristics based on the observation of users' past experiences.

[59] See AMATO MANGIAMELI 2020, 57: "each subject can be classified and each new device collects data, from the like it can be traced back to the color of the skin with minimal margins of error. With sexual orientation, political affiliation, as well as IQ, religion and much more, it happens that algorithms generate more and more personalized messages and stratagems to guide behavior".

[60] RODOTÀ 2004, 143: "the self becomes multiple, fluid, it is built in continuous interaction with machines (...) Thus by navigating the networks, everyone can encounter their own "double". In every sense, identity becomes nomadic". It becomes, as LE BRETON 2002, 7 writes, "a personal construction, a transitory and manipulable object, susceptible to multiple metamorphoses according to individual desires".

[61] See LYON 1997, 123.

According to *Deleuze,* "*marketing* is now the instrument of social control", which certainly appears as the most pervasive of the post-panoptic surveillance tools and embodies the *proprium* of hyper-productive capitalism[62]. The Fordist factory has given way to capitalist enterprise, which mainly deals with producing and selling services, knowledge and information. Moreover, in the information society based on the *value* of "data" and its *power,* it reveals itself not only as a new commodity of exchange, but also as an *individualizing* element. The collection of all data, starting from biometric data, understood in their broadest sense[63], such as data referring to the physical, physiological or behavioural characteristics of a person, which allows or confirms their unique identification, constitutes the capital of the new producers of information.

And if data represents the true resource of the digital market today, collection and processing (*data processing*) constitute its most characteristic activities. In this direction, the use of calculators or automated processors (i.e., computers) has contributed greatly, proving to be precious data accumulators as thinking and *intelligent machines* capable of communicating with humans but also with each other[64].

---

[62] See DELEUZE 2000, 238-239: "But, in the current situation, capitalism is no longer oriented towards production (…). It is a capitalism of hyperproduction. It no longer buys raw materials or sells finished products: it buys finished products or assembles separate parts. It wants to sell services and it wants to buy stocks. It is no longer a capitalism for production, but for the product, that is, for sale or for the market".

[63] See 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) or **GDPR.**

[64] AMATO MANGIAMELI 2020, 48-49: "And while ever more refined devices were being built, a debate has been activated on the intelligence of the computer (...) and the image we have of the gradually changed machine: first 'conductor and transmitter of power', now 'transformer of information'".

Their ability to collect, analyze, process, store and transfer a large amount of data is exponential[65]: through *data mining* techniques[66], the raw data becomes organized and accurate information which allows the monitors to continuously profile the user and exchange the *data*, as a new *res* or a legal object of commodification and negotiation[67].

This fuels a *data economy* based on the economic/commercial power of data which constitutes the object of the *new digital economy*[68]. Within this system, *Big Data*[69] proves to be extraordinarily fruitful with respect to new forms of surveillance and allows us to first market and then profit from the accumulation of data captured according to the typical logic of capitalist dynamics.

---

[65] AMATO MANGIAMELI 2020, 57: "Computers capable of learning automatically constitute the truly great turning point and with it highlight the possible risk of an uncontrolled system, such as to require a sort of Algorithm Liberation Front to make the decision-making criteria underlying the various tools transparent".

[66] See SORO 2019, 46.

[67] See MANGIAMELI 2023, 451: "the information circulating online is reified (data) and has become goods, in the legal sense, that is, 'things that can form the object of rights (art. 810 c.c.)' and as such, the object of economic activity, due to accessibility, of their specificity and their limitations".

[68] In an interview with Antonello Soro, President of the Guarantor for the protection of personal data on 6th June 2018 "We protect data, it is our life", he states that "data is the new oil. Data, the protagonist of digital society, is that element that is collected from every part of the planet and which is concentrated in large computers of a few companies. Here it is processed and the profiles of users are formed to whom targeted advertising is directed, and not only for commercial purposes, and today the wealth of"; SORO 2018, 16.

[69] See SARACENI 2023, 41: "big data are assembled thanks to the traces left by the user of a digital service who, in a more or less conscious manner, shares his/her ideas, habits and preferences, while browsing the internet and using its sites, search engines, bring them; they are also made up of the results coming from commonly used electronic equipment, capable of connecting to a site or a database. We note how, in this second case, the user participates in a very spontaneous and almost completely unaware way in the production of the data, given that it is his behavior that is tracked".

It is no coincidence that *Shoshana Zuboff*, analyzing the transformations and socio-economic consequences caused by the advent of the *digital age*, speaks of *surveillance capitalism* or a new form of surveillance that "appropriates human experience using it as raw material to be transformed in behavioral data" [70] and, referring to *Karl Marx*'s old image of capitalism as a vampire that feeds on work, she states that "surveillance capitalism does not feed on work, but on every aspect of human life" [71].

This type of surveillance, which is mostly exercised by private powers, although not replacing the truly public and political one, is certainly predominant. The market and market relations today, constitute the indisputable space for the exercise of global economic power: the fluidity together with the irregularity of the rules that govern it facilitate the circulation of data intended to constantly *shape* the choices and decisions of end users[72].

In this way, a form of *future behavioral market*[73] develops. A market of which the users themselves are commodity categories or parts of a production process used by surveillance capitalists to create products or services. Such pervasive control activities, so much so as to predict consumer desires and even personalize the services to be offered, make use of the application of

[70] See ZUBOFF 2019,17-18: "Some of this data is used to improve products or services, but the rest becomes private behavioral surplus, subjected to an advanced manufacturing process known as 'artificial intelligence' to be transformed into predictive products capable of predicting what we will do immediately, soon and in a long time".

[71] See ZUBOFF 2019, 19.

[72] RODOTÀ 2004, 137: "In the world of consumption and market logic, surveillance does not in fact have the objective of preventing or discouraging certain behaviors. These may prove to be completely foreign or indifferent purposes for those who systematically collect information: indeed, the interest is usually to ensure that consumption behaviors are repeated as much as possible".

[73] ZUBOFF 2019, 18.

need-to-know[74] techniques, which fuel the market of profiles (*commodification*) [75] and forecasts[76]. A surveillance built on private knowledge and predictions and, in fact, on an *instrumentalizing* power, which structures and exploits behavior, in order to modify, predict, monetize and control it[77].

Faced with this reading, cloaked in a certain skepticism, one could object that the data transformation process follows objective and neutral criteria, considering the huge amount of information and the infinite variables that may exist. Moreover, *databases*, these enormous virtual containers (so-called *SuperPanopticon*), use a binary, disambiguous language that sets the data in a rigid way, perform statistical calculation operations and are therefore free, at least in principle, from prejudices.

In truth, as it has been observed, data is not objective[78] nor is the final product that their processing returns. Rather, what happens in the interval that separates observation from the collection and processing of data remains something unfathomable and unrecognizable by many. In fact, there are few people who have access to *Big Data* and even fewer who know the logic of algorithmic calculation, with the consequence that it is precisely commercial interests (far from objective and neutral) that convey the data. It is information, therefore, that creates and shapes the needs to which

---

[74] See PERRI 2020, 17: "through which information is forcibly directed towards certain objectives, thus creating a dangerous asymmetry between knowledge and power, which the user has no way of escaping".

[75] See CALENDA 2009, 66: "The main resource of this market derives from the transformation of personal data from use value to exchange value, the so-called personal data commodification, through the construction of electronic profiles and their personification".

[76] ZUBOFF states, 2019, 370: "This is the heart of darkness of surveillance capitalism: a new kind of commerce that re-imagines us with the gaze that gives it its power, mediated by its own means of behaviour modification".

[77] See ZUBOFF 2019, 370 e 378, for which this power "(s)is based on measurable actions, therefore it only cares whether what we do is accessible or not to its incessant operations of rendering, modification, monetization and control".

[78] See AMATO MANGIAMELI 2020, 58-59.

society adapts and indeed makes them its own, to the point of inverting the primordial logic of every society, according to which the demand for needs arises from below and not (as instead is) relentlessly heteroimposed, predicted and induced from above.

This constant interconnection of data through the use of large-capacity computers has been defined – by the Australian computer scientist *Roger Clarke – Dataveillance*[79], a neologism that reveals the new face of surveillance, which is implemented through the interconnection of data, the speed of Network and computing power, and exercises systematic control of the actions or communications of people (both individual and mass)[80] in which the "data" constitutes the raw material which, subjected to a manufacturing process, is aimed at building strategies of *marketing*. It seems that a further element must be added to all this. The more or less (un)conscious contribution of users contributed to determining the impressive development of *Dataveillance* and capitalist surveillance. A simple search on any search engine – Google, Yahoo etc., – the acceptance of cookies, the use of smartphones, purchases and payments on the Internet, the posting of simple likes, Twitter, the display of posts and our images, which betray preferences and habits, are not just simple traces of us, but they are raw material with which we supply the large capitalist surveillance industries which do what they can profit and benefit from.

---

[79] See CLARKE 1988, 499: Dataveillance is "the systematic investigation or monitoring of the actions or communications of one or more people. Whose primary purpose is, generally, to collect information about them, their activities, or their associations. And, potentially, the second aim is to dissuade the entire population from undertaking types of activities".

[80] See LYON 1997, 73 e 74: "As Clarke observes, however, a 'dossier society' does not need centralization, only data surveillance. All a surveillance company needs, is a range of personal data management systems, linked by telecommunications networks, equipped with a compatible identification scheme".

Theorists have coined the expression *Panopticomodity*[81], precisely to represent a type of surveillance generated by users through the conscious exchange and commercialization of personal data in the context of economic activities, and beyond. Very simply, tools such as *Facebook*, *Instagram*, *Tik Tok* prove to be extraordinary vectors of information and personal data voluntarily left available to hundreds of millions of users and, above all, to large IT multinationals (*Big Tech*) with the consequent excessive overexposure of one's person and of one's private life which, inevitably, transforms into a continuously public life[82], and the almost unconditional transfer of our data (so-called "*dataism*"), and their portability to those who are responsible for processing them.

This adhesion on the part of the users creates a form of *participatory surveillance*, no longer anchored to the hierarchical and fixed schemes of Foucauldian panopticism, but to the faster, horizontal, and widespread ones of the Internet. Here the supervisor is also monitored, in fact the sole use of the system or platform implies a mutual *exchange* of information[83].

An exchange that should mitigate the effects of a *one-way* surveillance and should represent the "good" part of it, since a participatory, mutual and shared control would give the user the possibility of monitoring the use of both public and private power[84]. So that the *data* would become a usable asset for everyone and especially for individuals, who, through its knowability, could modify certain behaviors, shielding or filtering their information thus protecting, if anything, identity, and *privacy*.

---

[81]See LYON 2006, 8-9, referring to this expression as the sharing or even transfer of one's personal and behavioural data in exchange for (apparently) free services.

[82] See RODOTÀ 2002, VII.

[83] See PERRI 2020, 25: "it is the typical operating scheme of social networks where, information originally published by the author of the first message is followed by a series of further messages coming from members of the same social network which, often, contain contextual and content information precious for reconstructing a specific path, nourishing a person's profile or knowing their history or orientations".

[84] See PERRI 2020, 25, note 64.

3. SURVEILLANCE AND FUNDAMENTAL RIGHTS: THE INDISPENSABLE CLAIM TO DATA PRIVACY

Stefano Rodotà in an essay from a few years ago entitled *L'avvento della Tecnopolitica* asks: "(what) is the fate of democracy in a time in which information and communication technologies redesign the places of politics, break down borders, deny the same constraints of space and time, erase ancient subjects and create new subjectivities?" [85]. A provocative and insidious question that inevitably calls upon the destiny and guarantee of rights, which remain affected by the pervasive effects of *surveillance* in general and *technological* surveillance in particular[86].

The question, which is as old as the history of forms of control over the individual and the masses, is extraordinarily current and much more complex than in the past. The new models of surveillance and the transformations that have occurred in the relationship between State and citizen or between Authority and freedom must be taken into account. It is, therefore, undoubtedly more urgent that the problem of the protection of fundamental rights arises again today: where surveillance deconstructs identities, subjectivities, and politics; where it homologizes, conforms and profiles, it is necessary to imagine further paradigms of protection for rights, so as to restore substance to personal identity and the inalienable claim to one's *privacy*[87].

---

[85] See RODOTÀ 2004, 3: "If these are the effects of change, then it is not just a particular political form that is at stake. It is the entire society that, day after day, discovers itself continually changing. And with it, rights and languages, the very ways of building personality, change their meaning".

[86] RODOTÀ 2005.

[87] See PROSIA 2023, 375: "The term privacy (...) is (...) synonymous with intimacy, solitude, anonymity and/or confidentiality of private and family life, as well as a limit on the

In this regard, it does not seem, without significance, to have so far outlined the *consistency* of the new models of social control and to have highlighted their pervasive scope which, by penetrating people's lives, significantly alters the exercise of their rights, undermines the principle of equality to the point of touching the chords of human dignity, which remains the constitutional foundation of confidentiality and protection of personal data[88]. Think about the use of so-called biometric data collected even with just a *selfie* and capable of tracing a person's physical, physiological, and behavioral characteristics, allowing, or confirming their identification[89].

The immediate repercussion on individual freedoms and on the right to *privacy* – understood here, in its most specific meaning of *Recht auf informationelle Selbstsbestimmung* – (i.e., the right to informative self-determination)[90] is so evident that, on the one hand, it does not require

---

dissemination of information concerning a person, in the absence of his consent or other prerequisite of legitimacy".

[88] Human dignity, according to the interpretation of the Italian Constitutional Court, is "a value of absolute priority and of a fundamental nature in the scale of values expressed by the constitution"; "fundamental value", "purpose of the system", "constitutional value which permeates positive law", "value placed by the constitution at the basis of the rights of the person", "supreme value": Constitutional Court sentences of 19th December 1991, n. 467; December 10th, n. 1987; 24th May 1985, n. 161; 17th July 2000, n. 293; 5th February 1992, n. 37; 19th November 1991, n. 414.

[89] Biometric data are defined as special categories of personal data (art. 10), par. 1, EU Directive 2016/680.

[90] BVerfGE 15 dicembre 1983. With this expression the Bundesverfassungsgericht introduces a new concept which no longer includes only the protection of the private sphere (Sphärentheorie) but also the impact on the rights of the interested party of any processing of personal information and the consequent necessity that any such processing, to be legitimate, has its own specific legal basis. Accepting this perspective, the Karlsruhe Judges stated that "*Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses" Datum mehr. Wieweit Informationen sensibel sind, kann hiernach*

further arguments on the other hand, it requires a reflection that brings together the needs of surveillance with those of respect for the person and the confidentiality of their data.

In this regard, there have been various protection measures that legislators have deemed necessary to adopt. Going in this direction is the recognition in art. 8 ECHR, of the broader right to private (and family) life of the individual; the adoption of European Regulation 2016/679 (GDPR), *relating to the protection of natural persons with regard to the processing of personal data*, *as well as the free movement of such data*, which in addition to having harmonized the regulation within the EU, has recognized data protection as a fundamental right, the guarantee of which is achieved through strict and rigorous control over its processing, strengthened by forms of *accountability*. And, as regards Italy, the adoption with legislative decree no. 196 of 2003 of the *Code regarding the protection of personal data*.

Even more relevant, in this sense, however, was the contribution of jurisprudence which at various levels contributed to clarifying and strengthening the guarantee of the *Recht auf informationelle Selbstsbestimmung*. The violation of confidentiality understood, not only in the terms of the *Right to be let alone*[91], but also as the right to the protection of one's personal data, has given rise to a lively dialogue between the different jurisdictional levels – particularly revived after *Edward Snowden's* revelations (so-called *Datagate*) – at the center of which the protection of fundamental rights remains the indispensable claim against any illegitimate expropriation of one's personality by invisible digital controllers.

---

nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs: Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungs- und Verwendungsmöglichkeiten bestehen, läßt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten".

[91] According to the famous statement of a United States Supreme Court judge, it is the "right to be left alone (which) is in fact the beginning of all freedom", U.S. Supreme Court **Public Utilities Comm'n v. Pollak, 1952.**

In particular, the ECHR Court ruled on mass electronic surveillance measures[92], while not deeming similar measures incompatible *ex se* with the Convention – and indeed stating that mass interception of foreign communications constitutes "a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime" [93] – considered that the same, at least in the specific case, did not comply with the principles of necessity and proportionality pursuant to art. 8 of the Convention[94].

More specifically, on the use of facial recognition techniques[95], the Strasbourg Judges recalled that "The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention" and that the systematic or permanent recording of an individual's personal data may constitute an interference in the latter's

[92] ECtHR, 4 December 2015, Case Zakharov v. Russia, rec. n. 47143/06; ECtHR, 25 May 2021, Case of Big Brother Wacht and Others v. United Kingdom, rec. n. 58170/13, 62322/14 and 24960/15.

[93] ECtHR, 25 May 2021, Case of Big Brother Wacht and Others v. United Kingdom, rec. n. 58170/13, 62322/14 and 24960/15, 86.

[94] ECtHR, 25 May 2021, Affaire Centrum for Rättvisa v. Suede, rec. n. 35252/08, here too the Court recalls that "Il ne fait aucun doute (…) que l'interception en masse est d'une importance vitale pour les États contractants, qui en ont besoin pour détecter les menaces pesant sur leur sécurité nationale", however in the present case "le régime suédois d'interception en masse excède la marge d'appréciation accordée aux autorités de l'État défendeur à cet égard. Elle rappelle que l'interception en masse recèle un potentiel considérable d'abus susceptibles de porter atteinte au droit des individus au respect de leur vie privée. Eu égard au principe de la prééminence du droit, laquelle est expressément mentionnée dans le préambule de la Convention et inhérente à l'objet et au but de l'article 8 (…), la Cour estime donc que le régime suédois d'interception en masse, considéré dans son ensemble, ne contient pas de «garanties de bout en bout» suffisantes pour offrir une protection adéquate et effective contre l'arbitraire et le risque d'abus".

[95] ECtHR, 4 July 2023, Case Glukhin v. Russia, rec. n. 11519/20.

private life, especially if it is the image taken of a person, an image which constitutes one of the main attributes of his personality[96].

The Strasbourg Court paused on further occasions to reiterate that the development of information technology and the expansion of the possibilities for processing personal data, due to automation, places the protection of privacy and the protection of personal data in close relation, this the ultimate expression of the protection of personal autonomy from excessive interference by private and public entities[97]. And more effectively it declared that "The public interest cannot be reduced to the public's thirst for information about the private life of others, or to an audience's wish for sensationalism or even voyeurism"[98].

On the other hand, the Court of Justice of the European Union has also measured itself over time with the issue of the protection of personal data,

---

[96] While reiterating that "any interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which paragraph 2 of Article 8 refers, and is necessary in a democratic society in order to achieve any such aim". The Court concluded that "In such circumstances, the use of facial recognition technology to identify the applicant from the photographs and the video published on Telegram – and *a fortiori* the use of live facial recognition technology to locate and arrest him while he was travelling on the Moscow underground – did not correspond to a "pressing social need. In the light of all the above considerations the Court concludes that the use of highly intrusive facial recognition technology in the context of the applicant exercising his Convention right to freedom of expression is incompatible with the ideals and values of a democratic society governed by the rule of law, which the Convention was designed to maintain and promote. The processing of the applicant's personal data using facial recognition technology in the framework of administrative offence proceedings – first, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him while he was travelling on the Moscow underground – cannot be regarded as "necessary in a democratic society". There has accordingly been a violation of Article 8 of the Convention".

[97] ECtHR, 16 February 2000, Case *Amann v. Switzerland*, rec. n. 27798/95; ECtHR, 6 April 2010, Case *Flinkkilä and Others v. Finland*, rec. n. 25576/04.

[98] ECtHR, 8 November 2016, Case Magyar Helsinki Bizottság cv. Hungary, rec. n. 18030/11.

testing all its complexity and moving within a rather fragmented legal framework, and only partially recomposed by the provision contained in art. 16 of the TFEU (*ex* article 286 of the TEC), which establishes that "Every person has the right to the protection of personal data concerning himself" and by art. 8 of the *Charter of Fundamental Rights of the European Union* which consecrates the long process of codification of the right to *privacy* of which the protection of personal data now constitutes an autonomous right.

Thus for example, the European Judge stated that "to the extent that the activity of a search engine may affect (...) fundamental rights, privacy and the protection of personal data, the operator of that search engine (as responsible for data processing) must ensure (...) that said activity satisfies the requirements of Directive 95/47, so that the guarantees provided for by the latter can fully develop their effects, and effective and complete protection of individuals can actually be achieved for the interested parties, in particular the right to respect for their private life"[99].

In the words of the European Judge, we further read that in case of violation of personality through content published online on an Internet site, the injured person can bring an action for compensation before the courts of the Member State of the place of establishment of the person who entered this information[100]. And that, in any case, the needs of democratic control cannot overwhelm the fundamental right to privacy of natural persons, the principle of proportionality, defined as the cardinal principle of the protection of personal data, must always be respected[101].

In the footsteps of these indications, also at a national level, the legitimacy judges have reiterated the fundamental importance of protecting the privacy

[99]CJEU, 13 May 2014, Case Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12.

[100]CJEU, 25 October 2011, Case eDate Advertising GmbH v. x; Oliver Martinez, Robert Martinez v. MGN Limited, C-509/09 and C-161/10.

[101]See CJEU 20 May 2003, C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk and Others and 9 November 2010, C-92/09 and 93/09, Volker und Markus Schecke and Eifert.

of the individual through the protection of their personal data. The Italian Constitutional Court in sentence no. 20 of 2019, concerning the case of the *online* publication of the income and asset data of public administration managers, referred on several occasions to European and international jurisprudence, reiterating that "the right to the confidentiality of personal data, as a manifestation of the fundamental right to the intangibility of the private sphere, concerns the protection of the life of individuals in its many aspects" and that "(i)n the current era, it is particularly characterized as the right to control the circulation of information relating to one's person"[102]. The protection of this right is entrusted to the canons already developed at a European level and, in particular, to those of proportionality, relevance and non-excess. The Judge of Laws further observes that the rights to privacy and transparency are today called upon to face each other within the new digital scenario: "a context in which, on the one hand, personal rights can be placed in danger by the indiscriminate circulation of information, and, on the other hand, the wider circulation of data can better allow everyone to inform themselves and communicate". Even in the wake of this reasoning, accepting the question of constitutionality raised, it nevertheless held that "The indexing and free traceability on the web, with the aid of common search engines, of published personal data is not consistent with the aim of favoring correct knowledge of the conduct of public management and the methods of use of public resources. These forms of advertising rather risk allowing the "random" retrieval of personal data, also stimulating forms of research inspired solely by the need to satisfy mere curiosity"[103].

In the same direction, the Court of Cassation also underlined that the *employers' needs* (referring here to the work/business environment) cannot "assume such a scope as to justify a substantial cancellation of any form of

[102] Constitutional Court, 23 January 2019, sentence. n. 20 of 2019.

[103] Constitutional Court, 23 January 2019, sentence. n. 20 of 2019, point 5.3.1.

guarantee of the dignity and confidentiality of the worker" [104], so that the protection of one's personal data becomes, in the era of "*dataism*", an absolute priority as it concerns "the intangibility of one's social projection" and a "faithful and complete representation of the individual personality of the subject within the community, general and particular, in which this personality developed, expressed itself or solidified"[105].

Even some decisions of the *Bundesverfassungsgericht* appear particularly interesting, as they showed a certain sensitivity and great interpretative clarity regarding the protection of personal data even before it became a central topic of reflection for the doctrine. Already at the beginning of the 1980s, the decision with which the concept of *Recht auf informationelle Selbstsbestimmung* was introduced for the first time was of significant importance, as the right of the individual to decide personally on the transfer and use of data that concern him, stating that: "*Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen*" (par. 147).

But no less interesting were his subsequent pronouncements. With the ruling of 27th February 2008[106], the German Constitutional Court declared unconstitutional the *Gesetzes über den Verfassungsschutz* of the Land Nordrhein-Westfalen, which authorized the secret services (*Verfassungsschutzbehörde*) to access computer systems without the knowledge

[104] *Ex multis* Court of Cassation, 13 May 2016, n. 9904; Court of Cassation, 1st January 2012, n. 16622.

[105]Court of Cassation, 26 June 1986, n. 3769, which further states that this right implies that one's intellectual, political, social, religious, ideological, professional heritage must not be "altered, misrepresented, obscured or contested externally".

[106] BVerfGE, 27 febbraio 2008, 1 BvR 370/07, 1 BvR 595/07.

of the interested parties and to secretly intercept information from the Internet communications. On this occasion, *the right to confidentiality and integrity of information technology systems* is recognized (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*), so secret access to computer systems constitutes, for the *Karlsruhe* Judges, the violation of the more general personality law (art. 2, Abs. 1, GG).
The recognition of this right, applicable to systems which, alone or through their network connection, may contain personal data of the interested party, protects against forms of access that could reach essential parts of his life or personality[107]. Of similar tenor, and also relevant for the purposes of our discussion, at least three other decisions appear: the first of 24th January 2012[108], with which the German Constitutional Court held that some provisions of the *Telekommunikationsgesetz-TKG* were not compliant with the Constitution due to violation of art. 1, Abs. 1 GG and therefore, also, of the *informationelle Selbstbestimmung*; the second of 20th April 2016[109], with which it established that covert surveillance measures, and in particular the use of IT means that allow the acquisition of data "remotely, are incompatible with the compliance of fundamental rights and has identified proportionality as the principle by which to carry out the balancing *test* between public needs and the right to protection of personal data; the third of 19th May 2020[110],

[107] See par. 203: "Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist hingegen anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten".
[108]BVerfGE, 24 January 2012, 1 BvR 1299/05.
[109] BVerfGE, 20 April 2016, 1 BvR 966/09, 1 BvR 1140/09. The subject of the constitutionality judgment was the Bundeskriminalamtgesetz (BKAG).
[110] BVerfGE, 19 May 2020, 1 BvR 2835/17, concerning the Gesetz zur Ausland-Ausland Fernmeldeaufklärung des Bundesnachrichtendienst of 2016.

in which the German Law Judge, after recalling that the power of surveillance due to technological evolution and the intensity of communications taking place via the *World Wide Web* pervades every aspect of our daily lives, stated that "*Die Bindung der deutschen Staatsgewalt an die Grundrechte nach Art. 1 Abs. 3 GG ist nicht auf das deutsche Staatsgebiet begrenzt. Der Schutz der einzelnen Grundrechte kann sich im Inland und Ausland unterscheiden. Jedenfalls der Schutz des Art. 10 Abs. 1 und des Art. 5 Abs. 1 Satz 2 GG als Abwehrrechte gegenüber einer Telekommunikationsüberwachung erstreckt sich auch auf Ausländer im Ausland*".

Well, considering the progressive regulatory and jurisprudential evolution, only just mentioned here, a *habeas data* has been identified which extends the principle of intangibility, originally linked to personal freedom, to the *electronic body* which is the other dimension of contemporary man. This allows, at least in part, to create a protective barrier towards the indiscriminate collection, processing, and commodification of personal data, which *distorts* personal identity and builds a reflected image of our *digital twin*[111], in which we very often struggle to recognize ourselves.

4. FINAL CONSIDERATIONS

The scenery that appears before the disillusioned eyes of the *glass man*, as transparent as it is fragile, is a scenario that causes confusion. In the era we live in, can we really imagine the re-release of a (global) Big Brother?

Are we just victims of technological determinism or can we reverse the unstoppable movement of this new form of (*digital*) dictatorship and convert it, if anything, to the service of the person?

The questions are complex and identifying the answers is even more so. Certainly, faced with the arrogance of new forms of social control, it is necessary to proceed through a new understanding of surveillance that, first

[111] ROSSIGNAUD, DE KERCHOVE 2020, *passim*.

of all, enhances its ordering function, which still expresses the "good" side to be preserved and strengthened. There is no doubt that surveillance, as an instrument of security and political-social integration, as well as prevention (health, or energy-environmental), planning and regulation of the life of the State and the market would work for the benefit of man if only it was not governed as it is by technological power and, even more so, by ruthless capitalist logic.

Wherever it was thought to use IT progress to extend and exercise the power of surveillance indiscriminately, the liberal-democratic ideals of modern societies were repudiated. And the Internet, by lending itself to the game of the new supervisors – advantaged by the anomie of *cyberspace*, effectively confusing the absence of rules with the idea of absolute freedom[112] – has revealed its finiteness above all with regards to the protection of the freedom of the individual and, more specifically general, of his freedom of self-determination.

Moreover, also in light of what has already been reported, the "negative" implications deriving from the exercise of the power of control have become more evident precisely due to the help of new tools. It follows that even before surveillance, which remains a fundamental function of states, it is the *digital ecosystem* that must be regulated, relocating power and powers, surveillance, and Person that this allows within the context of the legal system.

"Law", as it is known, has an adaptive capacity in its DNA which continually pushes it to reconform in the face of the physiological changes in reality, first by incorporating them and then by ordering them and to deal "with the most diverse times and spaces"[113].

Anyone who objects that the Internet and Law (like the Sea and the Earth) are worlds distant from each other ignores that they are actually destined to enter into a mutual connection just for the most banal circumstance that

[112] MANGIAMELI 2023, 453.
[113] GROSSI 2006, 43.

everything that happens in virtual space is refracted inevitably on the real dimension, to the point that between the two worlds there is such an imbrication that cannot do without the intervention of law and national states[114].

If this is the direction in which to move, it seems that the natural place to bring this *together* is not simply the State tout court, but the constitutional State of law with its characteristics and, along with it, its law with its ordering and respect of fundamental rights[115]. In fact, recognizing that the State has the power to regulate the network and technology may, in itself, not be enough, as shown by those States that use technology to surveil and target opponents of the regime, and that often repress their own population, precisely by limiting the access to the network. It is therefore necessary for the State to become the bearer of the "new digital rights" that it itself and its system place the human and virtual person at the center, with respect to which every form of power acts legitimately only in a serving position[116].

In 1996 *John Perry Barlow*, a staunch supporter of the Internet, in his famous *Declaration of Independence of cyberspac*e, claimed the autonomy of the Internet and its extraneousness to politics and law. In the name of the future, he asked the governments of the industrial world to leave *cyberspace* alone, an original order, whose discipline could not depend on the institutions of the physical world. That is, a space capable of self-regulation and which did not require heteronomous rules, impervious to governments and rules.

However, the systemic limits of self-regulation[117] have been echoed by the request for legal discipline of the Internet, capable of containing its fragmentation and of ordering, with certain rules, the web of relationships that daily blossom within the folds of the fluid spaces that it generates. The requirement does not need to be explained. Relationships and legal

[114] MANGIAMELI 2023, 451.
[115] MANGIAMELI 2023, 1.
[116] GROSSI 1991, 135 ss.
[117] BUSCH 2019, 115 ss.; RODOTÀ 2010, 337, speaks of "attacks on online freedom".

relationships arise on the Internet every day, illicit and illegal conduct occurs, undue interference in violation of rights and freedoms. And it is precisely in the "pathological" moment that the self-regulatory model has proven to be incomplete, inadequate, often untimely and in need of being integrated with a model of *political* regulation.

The marriage between Law and the Internet was not so immediate: the initial prevalence of private regulation "miniaturized" the regulatory intervention of public authorities, resulting in an insidious recessive effect of Law. Faced with this setback, the idea has been put forward of building a regulatory model based on a *lex informatica*[118], i.e., on a system of automated and self-applicative technological rules universally valid for the access, use and circulation of information in virtual space. A system made up of technical rules which, with appropriate computational processes, regulates the functioning of the virtual space, although not in a completely neutral way.

Yet, evidently, this was not enough (and it is not enough) for the Internet or even for the *lex informatica* itself, to become an authentically legal rule. In fact, the regulation of the Internet requires to be integrated with properly legal rules, an expression of public decision-making power. Only the intervention of the Law and, for it, of the legislators of the different levels of government can guarantee the *cyberspace* to continue its development in a direction that aims to become an effective space for the realization of the needs of the human person.

Upon closer inspection, the Internet is nothing other than the projection of the dominion of the States which, although "tired giants of flesh and blood", retain a role of regulation and controllability of virtual space, which cannot be abdicated in favor of the flowering of a new *lex mercatoria,* or even *sectoral constitutions* (according to the Teubnerian idea), which would reflect particular interests driven by the cold logic of typically negotiated and

[118] REIDENBERG 1998, 553.

economic relations[119]. If this were not the case, the specter of a digital neo-feudalism[120] would re-emerge accompanied by the regression of the principles of the constitutional state of law and, moreover, by the risk of the privatization of public power.

If, therefore, one had doubted the ordering function of the Law, one would have fallen into the error of considering the *digital ecosystem* a completely self-referential, anarchic, unreal, a-political space, and completely subservient to the rules of private powers. Evidently this is not the case. Any new space is not unattainable for law. The airspace and then the maritime space have already demonstrated that they are not resistant to legal regulation. In fact, it belongs to the essence of Law itself to juridify relations and relationships, even virtual ones that arise and develop within immaterial spaces[121].

It follows that the legal regulation of cyberspace brings with it the regulation of surveillance power which, like any other power, must be legitimate and this condition cannot be imagined disconnected from the Law (and the State). Every power, as we know, needs law to legitimize itself. And consequently, social control is also unimaginable in the absence of institutional structures and rules that structure it, conform it, and ensure its functioning.

In addition to being legitimate, this power must also be *limited* and brought back within the coordinates of the constitutional state of law according to

---

[119] MICHETTI 2021, 151.

[120] RODOTÀ 2010, 347; D'ANDREA 2002, 77; VENANZONI 2020, n. 3.

[121] MANGIAMELI 2023, 452 ss.; MENTHE 1998, 69 (85): "After all, one could hardly posit three more dissimilar physicalities – the ocean, a continent, and the sky. What makes them analogous is not any physical similarity, but their international, sovereignless quality. These three, like cyberspace, are international spaces. As a fourth international space, cyberspace should be governed by default rules that resemble the rules governing the other three international spaces, even in the absence of a regime-specific organizing treaty, which the other three international spaces have".

the tradition of modern constitutionalism[122], which ensures its correct balance with the personalist principle. Therefore, it is up to the States, constitutionally conformed, and along with the international and supranational organizations that project the idea of constitutionalism beyond national borders, to use their sovereignty and their regulatory force beyond the fence of the traditional surveillance models, so that virtual space does not translate into a hidden space where new forms of control incompatible with the fundamental rights of the person nest. It is a question of building, through the agreement of these States, a fair and sustainable surveillance model, where the protection of personal identity is elevated to a necessary condition on which the organization of the entire society is based, and "the new paths of rights and citizenship, to root the attitudes of freedom in this dimension, and not the logic of "perverse" control"[123].

[122]MANGIAMELI 2023, 459: "Hence the unavoidable request from the people of the internet, towards private operators and governments, for a new regulation of cyberspace according to a typically constitutional projection, i.e., with reference to the protection of fundamental rights and democracy as well as other European values (art. 2 TEU), which requires the free exercise of freedoms, the prohibition of manipulation of the truth, the overcoming of the state of surveillance and the accumulation of data by private operators and governments and, above all, the prohibition of political use of data".
[123] RODOTÀ 2004, 145.

REFERENCES

AMATO MANGIAMELI, Agata C., *Diritto e cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Turin, 2000.

– *Educare alle nuove tecnologie. Qualche nuovo s/oggetto. Tra algoritmi, intelligenza artificiale, big data*, in AMATO MANGIAMELI, Agata C., CAMPAGNOLI, Maria Novella, *Strategie digitali #diritto-_educazione_tecnologie*, Turin, 2020.

– *Cyberspace* (entry), in AMATO MANGIAMELI, Agata C., SARACENI, Guido (eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

BARANZONI, Sara, VIGNOLA Paola, *Cosa potrebbe un corpo? Il dividuale e l'individuazione della filosofia contemporanea*, in *La Deleuziana – Rivista online di Filosofia*, 1/2015 – *Crisi delle Biopolitiche europee*.

BAUMAN, Zigmunt, LYON, David, *Sesto potere. La sorveglianza nella modernità liquida*, Bari-Rome, 2013.

BUSCH, Christoph, *Self-regulation and regulatory intermediation in the platform economy*, in CANTERO GAMITO, Marta, MICKLITZ, Hans. W. (eds.), *The Role of the EU in Transnational Legal Ordering. Standards, Contracts and Codes,* Cheltenham, 2019.

CALENDA, Davide, FONIO, Chiara, *Sorveglianza e potere*, Acireale, 2010.

CASTELLS, Manuel, *Il potere delle identità*, Bologna, 2014.

CIPOLLONI, Claudia, *The Right to anonymity. Overview of the Institute and Analysis of its Evolution in the Age of the Web Revolution*, in *Human(ties) and Rights. Global Network Journal*, 5, 2/2023.

– *Profilazione* (entry), in AMATO MANGIAMELI, Agata C., SARACENI, Guido (eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

CLARKE, Rogers, *Information Technology and Dataveillance*, 498-512, in *Communications of the ACM*, 31 May, 1988.

CURCIO, Renato, *Il capitalismo cibernetico. Dopo il panottico, oltre la sorveglianza*, Rome, 2022.

D'ANDREA, Dimitri, *Oltre la sovranità. Lo spazio politico europeo tra post-modernità e nuovo medioevo*, in *Quaderni fiorentini per la storia del pensiero giuridico moderno*, 31, 1/2002.

DANDEKER, Christopher, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*, New York, 1990.

DELEUZE, Gilles, *Poscritto sulla società del controllo*, in DELEUZE, Gilles, *Pourparler 1972-1990*, Macerata, 2000.

ESPOSITO, Mario, *Profili costituzionali dell'economia privata*, Padua, 2003.

FINN, Jonathan, "*Seeing surveillantly: surveillance as social practice*", in DOYLE, Aaron, LIPPERT, Randy, LYON, David (eds.), *Eyes Everywhere: The Global Growth of Camera Surveillance*, London, 2012.

FIORENTINI, Mario, *Sorveglianza* (entry), in AMATO MANGIAMELI, Agata C., SARACENI, Guido (Eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

FOUCAULT, Michel, *Sorvegliare e punire. Nascita della prigione*, Turin, 2014.

GIDDENS, Antony, *The nation-State and Violence*, Cambridge, 1990.

GROSSI, Paolo, *Prima lezione di diritto*, Rome-Bari, 2006.

GROSSI, Pierfrancesco, *I diritti di libertà ad uso di lezioni*, I, 1, II ed., Torino, 1991.

HELZEL, Paola Barbara, *Dataveglianza* (entry), in AMATO MANGIAMELI, Agata C., SARACENI, Guido (eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

KISSINGER, Henry, *Ordine mondiale*, trad. it., Milan, 2020.

LE BRETON, David, *Signes d'identité: tatouges, piercing et autres marques corporelles*, Paris, 2007.

LYON, David, *L'occhio elettronico. Privacy e filosofia della sorveglianza*, Milan, 1997.

– *Theorizing Surveillance. The panopticon and beyond*, Portland, 2006.

– *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milan, 2001.

– *The Culture of Surveillance. Wachting as a Way of Life*, UK, 2018; trad. it., *La cultura della sorveglianza. Come la società del controllo ci ha reso tutti controllori*, Rome, 2020.

MANETTI, Michela, *L'ordinamento giuridico fondato dalle piattaforme*, in LADU, Marco, MACCABIANI, Nadia (eds.), *L'individuo e la realtà digitale. Una questione costituzionale e democratica oltre la virtualità*, Naples, 2023.

MANGIAMELI, Stelio, *I diritti costituzionali dallo Stato ai processi integrativi,* Turin, 2020.

– *Stato, integrazione europea e globalizzazione. Le nuove sfide del Costituzionalismo*, *in Diritto e Società,* 1/2020.

– *Sovranità digitale* (entry), in AMATO MANGIAMELI, Agata C., SARACENI, Guido (eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

MARX, Gary T., *The Surveillance Society: The Treat of the 1984-Style Tecniques*, 21-26, in *The Futurist*, June 1985.

MARZANO, Michela, *Straniero nel corpo. La passione e gli intrighi della ragione*, Milan, 2004.

McGRATH, John, *Loving Big Brother. Surveillance Culture and Performance Space*, London, 2004.

MENTHE, Darrel C., *Jurisdiction in Cyberspace: A Theory of International Spaces*, in *Michigan Telecommunication and Technology Law Review*, 4/1998.

MICHETTI, Michela, *Organizzazione del potere e territorio. Legittimità dello Stato e livelli di governo*, Turin, 2021.

– *Sorveglianza* (entry), in AMATO MANGIAMELI, Agata C., SARACENI, Guido (eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

MUBI BRIGHENTI, Andrea, *Sorveglianza e teoria sociale*, in CALENDA, Davide, FONIO, Chiara (eds.), *Sorveglianza e società*, Rome, 2009.

NIGER, Sergio, *Sorveglianza e nuovi diritti di libertà*, in GALGANO, Francesco (directed by), *Trattato di Diritto commerciale e di Diritto pubblico dell'economia*, XLVIII, Padua, 2008.

ORTINO, Sergio, *Il nuovo Nomos della Terra. Profili storici e sistematici dei nessi tra innovazioni tecnologiche, ordinamento spaziale, forma politica*, Bologna, 1999.

PROSIA, Luigi, *Privacy* (entry), in AMATO MANGIAMELI, Agata C., SARACENI, Guido (eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

PARUZZO, Francesca, *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, Turin, 2022.

REIDENBERG, Joel R., *Lex informatica: The Formulation of Information Policy Rules Through Technology*, in *Texas Law Review*, 1998.

RODOTÀ, Stefano, *Prefazione*, in LYON, David, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, trad. it., Milan, 2002.

– *Tecnopoltica. La democrazia e le nuove tecnologie della comunicazione*, Rome-Bari, 2004.

– *Una Costituzione per Internet?,* in *Pol. dir.*, 3/2010.

ROSSIGNAUD, Maria Pia, DE KERCHOVE, Derrik, *Oltre Orwell. Il gemello digitale*, Rome, 2020.

RULE, James B., *Private Lives and Public Surveillance*, London, 1973.

SARACENI, Guido, *Big Data* (entry), in AMATO MANGIAMELI, Agata C., SARACENI, Guido (eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

SCHMITT, Carl, *Il nomos della terra. Nel diritto internazionale dello «jus publicum europaeum»*, trad. it., Milan, 1996.

– *Teoria del partigiano. Integrazione al concetto del Politico*, trad. it., Milan, 2005.

– *Terra e Mare. Una riflessione sulla storia del mondo*, trad. it., III ed., Milan, 2006.

SORO, Antonello, *Persone in rete. I dati tra poteri e diritti*, Rome, 2018.

– *Democrazie e potere dei dati*, Milan, 2019.

STAPLE, William G., *The culture of Surveillance*, New York, 1997.

SURACE, Marika, *Dalla sorveglianza moderna alla New Surveillance: il ruolo delle tecnologie informatiche nei nuovi metodi di controllo sociale*, in *ADIR*, *L'altro diritto*, 2005.

TOCQUEVILLE, Alexis, *La democrazia in America*, Milan, 1992.

TRAVERS, Guillaume, *La società della sorveglianza. Fase ultima del liberalismo. Dopo il pass sanitario, è in arrivo un controllo sociale mondiale?*, Florence, 2016.

VENANZONI, Andrea, *Neofeudalesimo digitale: Internet e l'emersione degli Stati privati*, in *mediaLaws*, 3/2020.

ZUBOFF, Shoshana, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, trad. it., I ed., Rome, 2019.