FOREWORD

From a constitutional perspective, there are some scary buzzwords nowadays that feature digital society and that clash against the classic core of constitutionalism. They can be summarised with the terms "digital surveillance" [1] and "digital power", [2] which bring about threats to fundamental values, principles, freedoms and rights. Surveillance and power are certainly not a novelty, as evidenced by surveillance studies; [3] what is new is the massive and pervasive reach and capabilities enabled by today's digital technologies (with specific regard to artificial intelligence) in conjunction with neuroscientific and behavioural science advancements. This conjunction brings about multiple paradigm shifts.

First, there is a paradigm shift that deals with the actors and purposes. In the past, the binomial "surveillance power" was referred to the State with disciplinary aims ("à la Foucault") or, more in general, control goals ("à la Deleuze"). In recent years, thanks to the Internet and the daily use of digital networked devices, the surveillance activity is broad and spread out, with no territorial borders, and is mainly carried out by globalised corporations for reasons of profit. [4]

Second, there is a paradigm shift that concerns the raw material and basic brick on which this new digital enabled surveillance is built: It is represented by digital data. More than giving rise to "dataveillance", this extensive amount of data (Big Data) integrates a sort of new faith called *dataism*: a «widespread *belief* in the objective quantification and potential tracking of all kinds of human behaviour and sociality through online

---

[1] Doctrine on the issue is wide, and it suffices to quote J.M. BALKIN, *The Constitution in the National Surveillance State*, in *Minnesota Law Review*, Vol. 93, No. 1/2008, pp. 1 ff.; S. ZUBOFF, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, Profile Books, London, 2019, pp. 27 ff.

[2] O. POLLICINO, *Potere Digitale,* in *Enc. dir.*, V, 2023, Giuffré, Milan, pp. 410 ff.; A. BRADFORD, *Digital Empires. The Global Battle to Regulate Technology,* Oxford University Press, Oxford, 2023, pp. 33 ff.

[3] T. TIMAN, M. GALIČ, B.J. KOOPS, *Surveillance Theory and its Implications for Law,* in R. BROWNSWORD, E. SCOTFORD, K. YEUNG (eds.), *The Oxford Handbook of Law, Regulation and Technology,* Oxford University Press, Oxford, 2017, pp. 731 ff.

[4] *Ivi,* pp. 733 ff.

media technologies». [5] Thus, the data subject has begun to be treated like an object. He/she is an object of calculation, measurement, predictions and assessments carried out by automated sophisticated algorithms. [6]

Third, in contrast to physical surveillance, this algorithmically driven data processing is not only something especially complex to understand (for laypeople but, in some instances, when deep learning and neural network are concerned, also for programmers) but also something not so visible and overt, giving rise to a sort of subtle and opaque power, which is built upon the knowledge gained by cross-referencing and a combination of different types of data stemming from multiple sources. Thus, distant from the principle of transparency and participation, which are pivots of democratic decision making.

Fourth, a paradigm shift has occurred with reference to the borders of this surveillance activity since, for the first time, surveillance has gained a granular capability to enter what can be defined as one's cognitive processes, their way of functioning and, thus, that which has always been sheltered by secrecy and considered as the most intimate and inner part of a person. Not only that, but as deepened in our research, there is a circular and mutually improving interaction that occurs among the knowledge of people's cognitive processes gained by artificial intelligence, neuroscience and behavioural sciences. As such, personal autonomy is not only the object but also the target of this activity.

Against this framework, our research has curtailed one "section" among the different tools by means of which digital surveillance can be conducted. More specifically, it addresses profiling and targeting practices. In some cases, profiling and targeting go hand in hand: These are the more worrisome cases for two reasons. First, they strongly increase the vulnerability of a person with respect to his/her personal identity and autonomous self-determination. Second, they have not yet been adequately caught and tackled by the legal system due to the fact that their object and target (our cognitive processes) represent something that has usually been out of the reach of the law. [7] In other cases, profiling acts as the enabler of private or public assessments and decisions, introducing the risk of discrimination based on the profiled attributes that do not necessarily, as will be argued, fall within the category of the attributes protected under European Union (EU) antidiscrimination law. In this second case, as different from the first, since decisions and decision making are involved,

---

[5] J. VAN DIJCK, *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*, in *Surveillance & Society*, Vol. 12, No. 2/2014, p. 198.

[6] V. MOLASCHI, *Algoritmi e nuove schiavitù*, in *federalismi.it*, No. 18/2021, p. 207.

[7] As evidenced by J.E. COHEN, *Studying Law Studying Surveillance*, in *Surveillance & Society*, Vol. 13, No. 1/2015, p. 91, law usually does not consider «the relationship between surveillance and the development of situated subjects and communities».

procedural issues and consequent possible legal effects or impacts on persons come into play, which are things the legal system is accustomed to handling. Consequently, even though procedures are automated and carried out by algorithms, procedural safeguards and rights are the typical tools the legal system has provided. [8]

Along the path that unfolds through the following Chapters, our point of arrival and our claim is aimed at anticipating the threshold of public law concern in order to encompass one's cognitive process, and thus, the basis of one's autonomous self-determination and personal identity. As such, the door of a domain that has mainly been of private law concern is entered. More specifically, the purpose is to supplement the typical private law approach made of information notice, transparency for the validity of consent and consequent accountability of the data controller, which are focused on the single person, with a broader perspective that takes into consideration the amplitude of the consequences of profiling and targeting; an amplitude that overcomes the individual and achieves more "systemic effects" that from the personalistic principle go ahead towards the pluralistic principle and the correct functioning of democracy in which market dynamics play an essential role that can affect the form of the State as a whole.

Our claim does not imply that the invoked public law approach must lead to the rigid, static and formal implementation of new constitutional provisions that integrate existing charters, constitutions or declarations. Such a solution would not be fit for purpose with respect to fast-moving digital challenges. Our claim is rather for a legal intervention underlying a policy option that is constitutional in substance, giving rise to necessary and proportionate limits on abuses of power (public or private). The issue thus shifts on the threshold that makes profiling and targeting an "abuse" against personal identity and self-determination and, further, by their means, an infringement of the personalistic and pluralistic principles.

The route undertaken in the following Chapters is aimed at upholding a better understanding of the stakes and assessing the fitness of the safeguards implemented by the EU. For this purpose, the Chapters are articulated as follows. After an introductory part (Chapter I) that briefly recalls the basic "technological and scientific tenets" of profiling and targeting practices along with the regulator's approach to technological advancements, attention will be driven to the specific "technicalities" of profiling and targeting as well as their main use-cases (Chapter II). Thus, the focus will shift to the fundamental constitutional tenets that profiling and tar-

[8] As evidenced by G. DE GREGORIO, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society,* Cambridge University Press, Cambridge, 2022, p. 270, «within this framework, enhancing due process complements the relevance of human dignity and proportionality as expression of the constitutional values».

geting undermine (i.e., personal identity and self-determination, the basis of the correct functioning of democracy: Chapter III) and include the doctrinal debate on new neuro-rights, which is mainly raised by neurotechnology but is similarly extendable to profiling and targeting (Chapter IV). Finally, an overview will be embarked upon of how the EU has been attempting to address the issue of profiling and targeting, tackling them along with their possible manipulatory and discriminatory effects (Chapter V).