Caraceni M. G., 'Digital surveillance technologies. Ethical, anthropological and political issues' (2022) 1 EJPLT, 336-349.
DOI: https://doi.org/10.57230/EJPLT221MGC

EJPLT
ISSN 2704-8012



# Digital surveillance technologies. Ethical, anthropological and political issues.

MARIA GIORGIA CARACENI
Research Fellow of Fondazione Magna Carta of Rome
Doctor in Philosophy of Law

Abstract

*The article aims to show how, over the decades, the noble ideals underlying the technological revolution began in the last century have been betrayed. The peculiar characteristics of that system defined as 'surveillance capitalism' by Shoshana Zuboff are first described, and then the historical and cultural framework allowing it to establish itself is reconstructed. Next, the consequences on human beings, such as the lack of privacy and the restriction of fundamental rights and liberties, are analyzed and discussed. Finally, the phenomenon of mass surveillance conducted through digital tools is addressed from a political and juridical point of view. In this regard, the risks that this represents for democratic political systems and the consequent legislative response that the European Union is trying to give are debated. Finally, conclusions are drawn.*

© The author(s) 2022, published by Suor Orsola Benincasa Università Editrice. This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Capitalism; Surveillance; Privacy; Democracy.

Summary: Introduction – 1. The Surveillance Capitalism. – 2. The historical context. – 3. New frontiers of surveillance. – 4. The expropriation of the self. – 5. Can we talk about digital totalitarianism? – 6. The risks for democracy. – 6.1 The case of social credit. – 7. The European legislative response. – Conclusions.

## Introduction.

Having to describe the so-called *technological revolution* that began in the last century, we might say that technological instruments appeared at their dawn as formidable tools that seemed to allow the human being to test a degree of freedom never experienced before: e. g., through the Web and storage devices, he has got 'the privilege of forgetting the various things he does not need to have immediately at hand, with some assurance that he can find them again if they prove important'.1 In a more and more complex and wealthy of information society, man inevitably struggles, because his memory is transient, so according to the theoretical conceptions, ideals, and motives underlying this evolution, technology would have made his life easier. Furthermore, it would have let him be able to weave personal relationships with extreme ease as well;2 and finally, thanks to the total and indiscriminate availability of information and the negligence of costs,3 it would have pushed in the direction of an increasingly radical democratization of society.4

## 1. The Surveillance Capitalism.

In someone's opinion, the dream of a fairer and more democratic digital future was shattered when the capitalist economic system realized the possibility that digital offered it. According to one of the most authoritative scholars of the subject, Shoshana Zuboff, to have discovered, put into practice, and spread that new form of capitalism that is defined as *surveillance*, was *Google*, a company founded in 1988 by Larry Page and Sergey Brin: users, guided by the ideal of information capitalism as a liberating and democratic force, immediately started using the search engine. These activities thus initiated to produce *new behavioral data*, which were initially randomly archived. Google engineers soon began to understand that this incessant flow

1 V Bush, 'As We May Think', *Atlantic* (Jul. 1954), 15, <https://mondodomani.org/eticaeinformatica/media/filelist/etistoinfa/1-%20Vannevar%20Bush%2C%20As%20We%20May%20Think%20%28completo%29.pdf> accessed 01 February 2022.

2 A similar idea is, e.g., expressed in the text of the presentation of *Community Memory*, the first kind of bulletin board considered the ancestor of modern forums, created in 1972 at the University of Barkley. See *Community Memory Message Base*, 1972, <https://web.archive.org/web/20130307110833/http://www.well.com/~szpak/cm/cmflyer.html> accessed 01 February 2022.

3 See V Bush, 'As We May Think', 8.

4 See G Salmeri, 'Il senso politico dell'informatica. Due esempi dalle sue origini', in A.T. Calogero Caltagirone (edited by), *Tecnologie della comunicazione e forme della politica*, Morcelliana, Brescia 2020, 237-40.

of collateral behaviors – or *behavioral surplus* –[5] was able to improve search engine performance; nonetheless, it is essential to emphasize that initially 'behavioral data were used for the benefit of the user, they offered value at no cost, and that value was reinvested in the user experience by improving services';[6] therefore, the raw material provided in data by users was collected and used to improve the speed and accuracy of searches and/or to contribute to the creation of secondary products such as the translator.[7]

Things have started to change as the new millennium dawned when extraordinary events occurred, modifying the nature of digital forever. First of all, the crisis that Google experienced in 2000 should be pointed out, when the company began to come under pressure from investors who were not satisfied enough with the revenues obtained through their financing. As in politics, the declaration of a state of emergency allows the implementation of exceptional measures that otherwise would not be justifiable, so, at the end of 2000, the state of emergency became a mantra for Google. It was the pretext for its founders to abandon any hostility towards *advertising* and cancel any spirit of reciprocity regarding the relationship with users. Brin e Page then hired the AdWords team to look for new ways to 'make money'.[8] From that moment on, Google began to work differently on and with the data collected in its immense archive, which from a technical point of view means that the *ads* would no longer be linked only to the *query* but *targeted* for the single individual. Google, therefore, opened its doors to advertising, but just to that *relevant* to users. However, this new rhetoric omitted a decisive aspect: Google would have entered a territory hitherto unexplored, exploiting the sensitive data revealed by its users. That raw material previously used to exclusively improve the quality of user navigation was therefore put at the service of targeted advertising. Thus, if Google had considered people as a goal in the first phase of its existence, now it was starting to consider them as a *means* to achieve a different purpose.

Hence, the *state of emergency* is the background on which the so-called *surveillance capitalism* took its roots. Google registered several patents in those years; particularly relevant is, for this discussion, the one recorded in 2003 and published two years later, called *Generating User Information for Use in Target Advertising*. The authors of the patent explicitly stated that their work was animated by a *profit-oriented logic*.[9] Here is Zuboff's comment about it:

> The techniques described in the patent imply that for each search conducted through the Google search engine, the system simultaneously presents a specific configuration of a particular ad and all of this in the fraction of time it takes to type the query. The data used to implement this instant translation of the query into the ad, a predictive analysis called

5 See S Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Rome 2019, 73-108.
6 Ibid 79 (translation mine).
7 See ibid.
8 K Swisher, 'Dot-Com Bubble Has Burst; Will Things Worsen in 2001?', *The Wall Street Journal* (Dec. 18th, 2000), <https://www.wsj.com/articles/SB97709118336535099> accessed 01 February 2022.
9 See K Barath, S Lawrence, M Sahami, *Generating User Information for Use in Target Advertising* (Jun. 16th, 2005), 1-2, pdf available at <https://patentimages.storage.googleapis.com/7c/39/51/a52b212d281f11/US20050131762A1.pdf> accessed 01 February 2022.

matching, went far beyond simply denoting search terms. New data sets, called user profile information or UPI, capable of drastically increasing the accuracy of these predictions, were complied. They would no longer have to guess, and there would be no more waste in the advertising budget. Mathematical certainty would take care of it.[10]

The system was gradually perfected thanks to the development of a series of mechanisms ranging from cookies to analysis methods up to predictive algorithms, according to a logic of expropriation of behavioral data as the basis of a new form of market that soon became dominant. Social networks – first of all, Facebook – certainly played a decisive role in this process, too, as they could rely on data voluntarily posted by users. 'We have better data than anyone else. We know the gender, age, location, and these are all actual data, not just inferred',[11] said Sheryl Sandberg – one of the top managers of Facebook and former creator of AdWords. Another fundamental invention in this sense is, for obvious reasons, represented by the *like* button.

While it is true that an economic system always produces specific social relationships,[12] *surveillance capitalism* embodies the asymmetry between knowledge and power that exists between a close circle of data experts operating in the dark, 'of which Google is the Übermensch',[13] and the rest of the individuals. If classical capitalism was born first from the expropriation of the land and then of the means of production,[14] that of surveillance was generated by an act of *digital expropriation*[15] in which *behavior* has become a *commodity*; however, users are unaware of the mechanisms of operation of this market because their consciousness is not just not necessary, but above all, it is not desirable. Surveillance capitalists, therefore, work to ensure that the protection of online privacy is cancelled and that any attempt at law that favors it is blocked, as it would pose a threat to their very existence.[16]

## 2. The historical context.

A question that seems legitimate to ask is: how did all this happen? At the beginning of the previous paragraph, mention was made of the circumstances that made it possible to implement and improve the system. However, the crisis that Google went through at the beginning of the new millennium cannot be sufficient to answer the question just posed. This business need was undoubtedly the trigger for an epochal change, but this could also happen thanks to particular cultural and historical conditions. First of all, the role that *neoliberal ideology* has historically played in the United States cannot be ignored: a study carried out by Jodi Short, law expert and academic at the University of California, aims to demonstrate how in the victorious defense –

10 S Zuboff, *Il capitalismo della sorveglianza*, 88-9 (translation mine).
11 See ibid 103 (translation mine).
12 See K Marx, *Il Capitale. Critica dell'economia politica*, Newton Compton, Rome 2015, 85-90.
13 S Zuboff, *Il capitalismo della sorveglianza*, 92 (translation mine, german original).
14 See K Marx, *Il Capitale*, 85-90.
15 See S Zuboff, *Il capitalismo della sorveglianza*, 110.
16 See J Brodkin, 'Google and Facebook lobbyists try to stop new online privacy protections', *Ars technica* (May 24th, 2017), <https://arstechnica.com/tech-policy/2017/05/google-and-facebook-lobbyists-try-to-stop-new-online-privacy-protections/> accessed 01 February 2022.

by Google and the other digital giants – of a territory within which being able to act outside the law, a liberal matrix can be identified; a particular convergence is then traced to the concept of *self-regulation*, according to which a company can independently decide its standards, check that they are respected and even issue a judgment on its conduct by applying 'the law to themselves, determine whether it has been violated, and voluntarily report and remediate legal violations': 17 it is in this context that the surveillance capitalists have developed a strong 'cyberlibertarian'18 ideology.

The other historical condition that allowed surveillance capitalism to assert itself can be identified in the sudden reorientation of government security policies that occurred in America as a consequence of the 9/11 attacks.19 After the 9/11 attacks, the political agenda changed abruptly, and the priority became security over privacy. Both the European Parliament and the US Congress presented bills expanding surveillance activities. 'The United States Congress passed the Patriot Act, devised the Terroristic Screening Program, and instituted a series of additional measures that vastly expanded the collection of personal information'. 20 There were then the institutions themselves that broke down every wall because they needed to draw on the information collected by the various digital agencies making user profiling activities.21

## 3. New frontiers of surveillance.

It is not just through online activities that users can be profiled. Intelligent appliances, now present in several homes, are, for surveillance capitalists, a precious means of collecting data (in many cases, users are forced to share data and grant permissions without which functionality is limited). 22 Digital assistants such as Cortana or Alexa can acquire complete data on people's lifestyle habits, being *conversation* the medium of interaction between the user and the device.23 They are even able to modulate their responses by basing them on the inflection of the interlocutor's voice, interpreting the more or less acute tone as a manifestation of a specific emotional state. However, smartphones provide the best data: most smartphone apps require user positioning even if it is not necessary for its operation, just as it is often necessary to grant access to the archive of files, photos, and videos. In particular, the apps that can extract the most sensitive data are those for health and fitness: they can monitor biometric data – such as heart rate, body temperature, sweating, blood pressure, calorie consumption – and require the

17 JL Short, 'The Paranoid Style in Regulatory Reform', *Hastings Law Journal* 63 (Jan. 12th, 2011), 667, pdf available at <https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1242&context=hastings_law_journal> accessed 01 February 2022.
18 S Zuboff, *Il capitalismo della sorveglianza*, 118 (translation mine).
19 See D Lyon, *Surveillance After September 11. Themes for the 21st century*, Polity, 2003, 7.
20 S Zuboff, *Il capitalismo della sorveglianza*, 124 (translation mine).
21 See § 6.
22 See S Zuboff, *Il capitalismo della sorveglianza*, 249-50.
23 See ibid 274.

user to reveal precise information in order to effectively develop customized plans that he can follow – for example, a diet.24

In 2016, more than ʿ100,000 apps dedicated to mobile health for Android and iOS (iPhone) operating systems [were available], which doubled over the last two yearsʾ.25 Furthermore, ʿIn the United States, most health and fitness apps were not subject to health privacy lawsʾ.26 In response to this, also in 2016, the Federal Trade Commission (FTC) issued guidelines that mobile app developers should follow in order to increase transparency, privacy, and security;27 however, they can be easily circumvented, possessing only a *vis directiva* and not a *vis coactiva*. Many studies are revealing how health-related mobile apps sell users' data to advertising companies without their permission;28 in particular, a survey on Android apps for diabetes appeared in the *Journal of American Medicine* in 2016 demonstrated that, ʿPermissions, which users must accept to download an app, [automatically] authorized collection and modification of sensitive informationʾ, 29 even those not voluntarily released by users: the apps, in fact, also accessed information regarding identity, call log, archive, contacts, wi-fi connections.30

Besides the various wearable devices and apps dedicated to health, social networks are also a mine to extract biometric data. For example, in 2017, Facebook declared that it had about two billion profiles – now five – through which 350 million photos were uploaded per day, and in 2018 it announced that it had achieved a face recognition capacity that reached a level of 97.35 percent accuracy,31 identifying facial recognition as a further possibility to improve ad targeting.

In 2015, the National Telecommunications and Information Administration (NTIA), under the patronage of the United States Department of Commerce, attempted to establish general guidelines for the creation and use of biometric information. After weeks of negotiations, NTIA had to ascertain; the impossibility of reaching an agreement due to the hard-line held by the technology companies – especially regarding the consent. So, in 2016 it had to

---

24 Biometric data can even be interpreted by digital technologies as a manifestation of a particular mood, such as detecting an increase in a heartbeat when a subject is exposed to viewing specific contents. See ibid 260-1.

25 G Addonizio, ʿThe privacy Risks Surrounding Consumer Health and Fitness Apps with HIPAA's Limitations and the FTC's Guidanceʾ, *Health Law Outlook* 9 (n 1, 2016), <https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1015&context=health-law-outlook> accessed 01 February 2022.

26 S Zuboff, *Il capitalismo della sorveglianza*, 263 (translation mine).

27 See Federal Trade Commission, *Mobile Health App Developers: FTC Best Practices* (Apr. 2016), <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices> accessed 01 February 2022.

28 A long series of studies proves this. See e.g.: Privacy Rights Clearinghouse, *Mobile Health and Fitness Apps: What are the Privacy risks?* (Jul. 1st, 2013); pdf available at <https://privacyrights.org/consumer-guides/mobile-health-and-fitness-apps-what-are-privacy-risks> accessed 01 February 2022. For further bibliographical information see: S. Zuboff, *Il capitalismo della sorveglianza*, 586 (nt. 50).

29 SR Blenner and others, ʿPrivacy Policy of Android Diabets App and Sharing of Health Informationʾ, JAMA 315 (n 10 2016), 1051; pdf available at <file:///C:/Users/User/Downloads/jld150059%20(1).pdf> accessed 01 February 2022.

30 See ibid.

31 See Y Taigman and others, ʿDeepFace: Closing the Gap to Human-Level Performance in Face Verificationʾ, *Facebook Research* (Apr. 14th, 2018) 7; pdf available at <https://www.cs.toronto.edu/~ranzato/publications/taigman_cvpr14.pdf> accessed 01 February 2022.

limit itself to presenting *recommendations*.32 However, the problem with this kind of document is that lacking regulatory value; they are not binding and can be ignored.

## 4. The expropriation of the self.

Digital surveillance is often justified by those who practice it with the rhetoric of *inevitability*: it is necessary to be constantly monitored as this increases social security. After all, those who have nothing to hide have nothing to fear: it was Google CEO Eric Schmidt who was the first to become the spokesperson for this concept.33 Faced with the incessant repetition, many people have come to accept it. In *Nothing to Hide. The False Tradeoff between Privacy and Security*, Daniel Solove reports some of the most common arguments given by people who were asked if they cared about their privacy and worried about the increasing use of digital devices for mass surveillance. Among the most common responses are:

I don't have anything to hide from the government. I don't think I had much hidden from the government in the first place. I don't think they care if I talk about my ornery neighbor.

Do I care if the FBI monitors my phone calls? I have nothing to hide. Neither does 99.99 percent of the population. If the wiretapping stops one of these Sep. 11 incidents, thousands of lives are saved.

Like I said, I have nothing to hide. The majority of American people have nothing to hide. And those that have something to hide should be found out, and get what they have coming to them.34

Actually, the *nothing to hide argument* not only proves to be logically inconsistent as 'arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying that you don't care about free speech because you have nothing to say',35 not only it does infringe a "right"36. It hides a contradiction since those who invoke it are ready to make an exception for themselves since surveillance practices are almost unknown

32 See S Zuboff, *Il capitalismo della sorveglianza*, 267-8.

33 'If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place': these are the words pronounced by Schmidt in an interview with Class CNBC on December 9th, 2009. The partial video of the interview is available on YouTube at the address <https://www.youtube.com/watch?v=A6e7wfDHzew> accessed 01 February 2022, while some of Schmidt's statements have been reported by the most important newspapers in the country; please refer, e.g., to the article published the next day by the *Huffington Post*, 'Google CEO On Privacy: "If You Have Something You Don't Want Anyone To Know, Maybe You Shouldn't Be Doing It"' (Dec. 10th, 2009), <https://www.huffpost.com/entry/google-ceo-on-privacy-if_n_383105> accessed 01 February 2022.

34 DJ Solove, *Nothing to Hide. The False Tradeoff between Privacy and Security*, Yale University Press, London 2011, 22.

35 This is the famous counter-argument formulated by Edward Snowden in response to that of "Nothing to hide". Part of the video of the first interview in which Snowden expressed his argument was published by A Rusdridger, J Gibson, E MacAskill, 'Edward Snowden: NSA reform in the US is only the beginning', *The Guardian* (May 22nd, 2015), <https://www.theguardian.com/us-news/video/2015/may/22/edward-snowden-rights-to-privacy-video> accessed 01 February 2022. We will return to Snowden in § 6.

36 The term "right" has been placed in quotation marks because it must be specified that there is no natural right to privacy in the American Constitution; however, jurists include it in the IV amendment. The same applies to articles 13, 14, and 15 of the Italian Constitution. The GDPR of the European Union talks about the right to the protection of personal data. For further information regarding the GDPR, see § 7.

to the most, but it is also patently *false*. In reality, privacy is a desire common to all as it is essential – and not an accessory – for the human being. The private sphere is where everyone feels free to act, think, speak as they prefer since they are away from the judgmental gaze of others. 'Privacy is a fundamental condition of being a free person'.37 The restriction of privacy limits the freedom of choice because when people know they are being watched, they change their behavior and try to do what others expect from them to avoid shame and condemnation. All oppressive political and religious authorities rely on the idea that the awareness of being observed induces a subject to comply with what is required: the re-educational method formulated by Jeremy Bentham in the *Panopticon* is its emblem. The occupants of the Panopticon were not necessarily under constant surveillance, but not being able to know for sure was enough.38 The same principle underlies the surveillance system described by George Orwell in *1984*.39 Michel Foucault in *Discipline and Punish*, commenting on the panoptic method, came to argue that omnipresent surveillance even pushes individuals to internalize their supervisors and therefore to do what is expected of them without realizing or not being controlled.40 Several studies show how awareness of being observed alters behaviors.41

Privacy is relational; it depends on whom you are dealing with: for example, having a job but looking for a better one is certainly not illegal or condemnable. However, it is understandable to have the desire that your employer does not come to know it. It could be said – provocatively – that *everyone has something to hide*.42 When an economic system such as the one described up to now is affirmed, which is based on the expropriation of sensitive data in order to profile each user and predict their behavior by showing them content that they will *indeed* consider relevant, it follows that the personal boundaries that protect the inner life are considered an obstacle to business. It is then the self itself, the interior space of lived experience within which each individual creates meaning and which is the foundation of freedom, to be exposed to the risk of disintegration because the human being cannot live without giving up meaning to his experience and cannot conceive himself as the result of predictions based on the analysis of accumulated data by monitoring his online activity, collecting his biometric data, listening to his conversations. Indeed, it is reasonable to predict that if someone ever had the chance to meet his "digital

37 G Greenwald, *No Place to Hide. Sotto controllo: Edward Snowden e la sorveglianza di massa*, Rizzoli, Milan 2014, 262 (translation mine).
38 See J Bentham, *Panopticon. Ovvero la casa d'ispezione*, Marsilio Editors, Venice 2009, see in particular 46-51.
39 See G Orwell, *1984*, Newton Compton, Rome 2021.
40 See M Foucault, *Sorvegliare e punire. Nascita della prigione*, Einaudi, Turin 2014, 194.
41 For example, an experiment conducted in 1975 by the psychologists of Stanford University entitled *The Chilling Effects of Surveillance: Deindividuation and Reactance*, goes in this direction. In this case, the participants were subjected to different levels of surveillance and were asked to express an opinion on controversial political issues. For example, regarding the legalization of marijuana, some were told that their answers would have been shared with the police: only 44 percent said they were in favor. However, the percentage of those in favor reached 77 percent among the individuals told otherwise. This experiment is mentioned in G Greenwald, *No Place to Hide*, 270-2. Moreover, the pdf of the entire study is available online at <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1002.4273&rep=rep1&type=pdf> accessed 01 February 2022.
42 See G Greenwald, *No Place to Hide*, 275.

avatar", he would not recognize himself because each individual attributes enormously excedent meanings to his singular story. Therefore, the freedom to create meaning cannot and must not be subtracted.

No matter how much it is taken from me, this inherent freedom to create meaning remains my last sanctuary. Jean-Paul Sartre writes that 'freedom is nothing other than the existence of our will', and explains: 'It is not enough to want, it is necessary, to want to want'. The birth of the will to will is the inner act that assures us of our nature as autonomous beings who project their choices into the world and exercise the self-determination and moral judgment necessary for civilization, of which they are the last bastion. (…) The deeper the prediction imperative is pushed into the self, the more the value of the surplus becomes irresistible, and the operations to capture it increase. What happens to the right to speak in the first person and as oneself when the frenzy to institutionalize activated by the imperative of foresight is trained to capture my sighs, blinks, pronunciation to reach my thoughts, and how to someone else's ends? It is no longer the surveillance capital that grabs the surplus of my searches, purchases, and Internet browsing. The surveillance capital wants something more than my space-time coordinates; it is violating the inner sanctum, with machines and algorithms that decide the meaning of my breath and my gaze, of the muscles of my jaw, of my voice that becomes higher, of all the exclamation marks I had typed with hope and innocence.43

## 5. Can we talk about digital totalitarianism?

Surveillance capitalism, this new type of trade, can be defined as 'instrumentalizing power (…) [which] has the task of *structuring and exploiting behavior in order to modify, predict, monetize and control it*'.44 Those who take sides against this new type of power – scholars, journalists, activists – often do so by recalling the Orwellian Big Brother and even more the specter of totalitarianism, to the point that the threat embodied by subjects such as Google, Facebook, and the entire commercial surveillance is often referred to as 'digital totalitarianism'. 45 However, comparing a new phenomenon to another one already known can be risky. Intellectuals had to elaborate new conceptual categories in order to frame and describe the unprecedented effects due to the totalitarian governments of the last century;46 the same

43 S Zuboff, *Il capitalismo della sorveglianza*, 306 (translation mine). The quotation in quotation marks is taken from JP Sartre, *Being and Nothingness*, Washington Square, New York 1993, 573.
44 Ibid 370 (translation mine).
45 See in this regard 'Move Over Big Brother', *The Economist* (Dec. 4th, 2004), <https://www.economist.com/technology-quarterly/2004/12/04/move-over-big-brother> accessed 01 February 2022; R Blakely, 'We Thought Google Was the Future but It's Becoming Big Brother', *Times* (Sep. 19th, 2014), <https://www.thetimes.co.uk/article/we-thought-google-was-the-future-but-its-becoming-big-brother-h3psqft8mpt> accessed 01 February 2022; C Doctorov, 'Unchecked Surveillance Technology Is Leading Us Towards Totalitarianism', *International Business Times* (May 5th, 2017), <https://www.ibtimes.com/unchecked-surveillance-technology-leading-us-towards-totalitarianism-opinion-2535230> accessed 01 February 2022. For further bibliographical information, please refer to S Zuboff, *Il capitalismo della sorveglianza*, 600 (nt. 1).
46 Several scholars have indicated the will to dominate the human soul among the peculiar characteristics of totalitarian regimes. See, e.g., CJ Friederich, Z Brzezinsky, *Totalitarian Dictatorship and Autocracy*, Harvard University Press, MA 1956; TW Adorno, *Education after Auschwitz*, in *Critical Models: Inventions and*

effort is needed in this historical moment: Shoshana Zuboff, as mentioned above, among others, essayed this undertaking.47 It, therefore, becomes a priority to get aware of the fact that the horizon in which what has been defined digital totalitarianism moves is utterly different from that within which twentieth-century totalitarianism took shape.

The instrumentalizing power moves in a different way and towards an opposite horizon. Totalitarianism used violence, while instrumentalizing power uses the means of behavior modification: this is where we need to change focus. The instrumentalizing power is not interested in our souls or in imposing principles. There is no training or transformation for spiritual salvation, no ideology to conform to our actions. The instrumentalizing power is neither interested in possessing the totality of a person nor in exterminating or torturing our bodies in the name of pure devotion. It appreciates [our] data [but] (…) does not aim for pain, bereavement, terror; however much it undoubtedly appreciates the behavioral surplus coming from affliction. It is profoundly and infinitely indifferent to what motivates us and what we consider significant. (…) Even if it does not kill, it is frightening, incomprehensible, and unprecedented, just as totalitarianism was for victims and witnesses. Our encounter with an unprecedented power helps us explain why it has been challenging to baptize and learn about this new kind of coercion. (…) Totalitarianism was a political project allied with economic power to subjugate society. Instrumentalizing power is a market power that converges with digital for a unique type of social domination.48

## 6. The risks for democracy.

The ambitious reform of everyday life outlined up to now has been carried out by private capital; this would not have been possible, however, if there had not been supported from public institutions: the *war on terrorism* 'legitimized the use of certainty produced by machines as a solution to social uncertainty. (…) In the sixteen years of the Bush and Obama administration, the "advancement of information technology" was considered "the most effective" response to the threat of terrorism'.49 Americans were allowed to learn what happened regularly in 2013, after Edward Snowden, a young computer scientist who had worked for the CIA and the NSA, made available to some *Guardian* reporters a series of documents revealing the architecture of the most significant security program mass surveillance ever conceived and

*Catchwords*, Columbia University Press, New York 1996; H Arendt, *Le origini del totalitarismo*, Comunità Editions, Milan 1996.

47 Among the most significant categories elaborated by Zuboff we point out the aforementioned *behavioural surplus* (see *Supra* § 1) and that of *rendering* conceived as the set of operations that intervene on the gap between experience and data to ensure that the first one is transformed in the second ones (see S Zuboff, *Il capitalismo della sorveglianza*, 247-9).

48 Ibid 377-8 (translation mine).

49 Ibid 401-2 (translation mine). Internal citations are reported by Zuboff and are taken from P Swire, 'Privacy and Information Sharing in the War of Terrorism', *Villanova Review* 51, n. 4 (2006), 951, pdf available at <https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1195&context=vlr> accessed 01 February 2022.

implemented.50 It was discovered that the National Security Agency (NSA) had forced every telephone company to provide printouts of all communications between American citizens and foreign countries, regularly acquired data from the giants of information technology and the Internet, spied on political leaders and competitors of American companies, accessed email texts, entered cell phones and computers around the world. Faced with the enormous scandal, American institutions tried to justify themselves by appealing to the rhetoric of "nothing to hide", concealing behind the increased security needs due to the threat of terrorism and stressing that 'many of the surveillance procedures described in the Snowden archive referred to the mere acquisition of metadata, 51 not contents', 52 as if these practices were less intrusive. Actually, if a government always knows who the recipients of a confident citizen's calls are, knows the times and duration, knows where they are made from and so on, it can collect much more information than it could by intercepting a single conversation. The are several experts who support this.53

### 6.1. The case of *social credit.*

Where can this trend lead? One possible answer is offered by *social credit*, a system developed – starting from 2015 – by the Chinese government for the purpose to leverage 'the explosion in personal data generated through smartphones, apps, and online transactions in order to improve citizens' behavior (…) [The system requires] Individuals and businesses [to be] (…) scored on various aspects of their conduct – (…) [such as frequented places, purchases, acquaintances] – and [then] these scores (…) [are] integrated within a comprehensive database that not only links into government information but also to data collected by private businesses'.54 Based on social and financial activities and biometric tracking – starting from fingerprints – subjects inevitably leave signs of their behavior, which are traced by a system that judges them as *good* or *bad* and consequently assigns them rewards and punishments. The purpose of the system is to induce them to adopt *only good* behaviors because, otherwise, the extent of the punishments will be so heavy

50 The story is detailed in the book above published by G Greenwald – one of the journalists contacted by Snowden – in which it is also possible to consult some extracts of the documents he had come into possession of thanks to the young computer scientist. See G Greenwald, *No Place to Hide*.
51 Google and other surveillance capitalists have often resorted to this same argument.
52 G Greenwald, *No Place to Hide*, 202 (translation mine).
53 For instance, Edward Felten, a professor of computer science at Princeton, in a sworn deposition in which the American Civil Liberties Union (ACLU) challenged the legality of the metadata collection program practiced by the NSA, brought various examples to support this thesis. In general, he believes that wiretapping is far more cumbersome acquiring metadata due to language barriers such as the use of jargon or coded signals that could – intentionally or unintentionally – obscure the meaning of the message. The transcript of his statements is available online: see The United Senate States, *Written Testimony of Edward W. Felten* (Oct. 2nd, 2013), <https://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf> accessed 01 February 2022.
54 R Creemers, 'China's chilling plan to use social credit ratings to keep score on its citizens', *CNN.com*, (Oct. 28th, 2015) <https://edition.cnn.com/2015/10/27/opinions/china-social-credit-score-creemers/index.html> accessed 01 February 2022. To consult the text of the law concerning the establishment of the social credit system, please refer to *State Council Notice concerning Issuance of the Planning Outline for the Construction of a Social Credit System* (2014-2020), GF n 21 (2014), <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/> accessed 01 February 2022.

that it will condemn them to social exclusion. Possible rewards include favorable conditions on loans and rentals, car rental without a down payment, greater visibility on dating websites. According to a *China Daily* article, blocked citizens as debtors or in default of a court order was prevented – for example – from taking the plane and the high-speed train and/or hiring – in the workplace – managerial roles. 55

Could this be an example of *digital totalitarianism*? Can a comparison be made with the world of *1984*? Answering these questions is not easy, but what we want to underline in the context of this discussion is the perceptible difference between Western surveillance capitalism and Chinese state surveillance. Although the means used to produce behavioral modification are the same at the basis of capitalism surveillance, the purpose of Chinese politics is quite different, it aims to achieve guaranteed results at a *social level* and not at a *market level*. However, on closer inspection, the logic behind this system is the same underlying websites such as eBay, Uber, and TripAdvisor, on which users are evaluated and thus acquire or lose value and credibility in the eyes of other users.

However, China is not a democracy; therefore, in our context, there is no reason to place too much emphasis on the social credit system. There is also another significant distinction between the West and the Chinese world: surveillance capitalism in the West is mature and offers its tools to the State, which necessarily needs to collaborate if it wants to access a specific type of power. On the other hand, in the Chinese context, the State has assumed a prominent role in transforming social assets because it is the owner of a political project – we repeat, not of a market one – which can only be achieved through an automated solution.

Europe is certainly not China, but it is necessary to be aware that there are phenomena worth dwelling on even in this part of the world. For example, in 2014, Italy established the Public System of Digital Identity, a Single National Number necessary for citizens to access the online services of the public administration. In addition, the electronic identity card contains a high-tech microprocessor in which essential biometric data such as the scanning of the fingerprints of the indexes and the facial pattern are stored. In France, since 2016, the Titres életronique sécurisé (TES) has been established, i.e., a system for centralizing the biometric data of the population – also, in this case, facial pattern and fingerprints – collected thanks to passports and identification cards in the perspective of integrating it with the missing ones. Finally, we want to refer to an experiment conducted in Sweden in 2018 by the Ministry of the Future on three thousand volunteers, consisting in the installation of a subcutaneous microchip between the thumb and forefinger of one of the hands, and it allows carrying out numerous operations such as payment by credit card, online purchases, booking air and rail tickets, managing house or car keys. 56

55 S Xiaofeng, C Yin, 'Court Blacklist Prevents Millions from Flying, Taking High-Speed Trains', *China Daily* (Feb 14th, 2017), <https://www.chinadaily.com.cn/china/2017-02/14/content_28195359.htm> accessed 01 February 2022.

56 These data are taken from R Curcio, *L'algoritmo sovrano. Metamorfosi identitarie e rischi totalitari nella società artificiale*, Sensibili alle foglie, Rome 2018, 103-6.

We conclude this paragraph with the following reflection: the Coronavirus pandemic – offering the formidable reason for containing infections – has justified the implementation of tracking and data collection systems (including biometric ones) and probably has acted in this sense an accelerator of a process which was already underway.

## 7. The European legislative response.

Starting from 25 May 2018, the European Union has taken a big step forward in the field of data protection with the adoption of a new General Regulation (GDPR, *General Data Protection Regulation*).57 Unlike directives, which must be transposed – through the adoption of national measures – by individual States and which are binding only on the objectives to be achieved – therefore not being mandatory in all their elements –, *regulations* are general. They aim to bring the legal institutions on specific subjects of the Member States as close as possible. Therefore, the Regulation mentioned above aims to respond to the modern need for sustainable development of technological dynamics and aims, through uniformity and simplification, to create a single data protection authority for all EU countries. The main goal of the GDPR is to establish the methods of processing and protecting the data of natural people and to protect their fundamental rights and liberties by establishing that all entities that collect data belonging to people residing in the EU comply with the established rules. The GDPR also introduces new rights for the owner – such as the right to delete data –,58 new obligations for companies that process data – such as the imposition of consent which must be granular, unambiguous, and expressed –,59 and penalties that may arrive up to twenty million or 4% of the company's annual turnover – if higher – in case of violation of specific articles.60 A further tool is also introduced to protect the data owner, namely the *complaint*, which allows you to contact the Privacy Guarantor directly and request verification by the Authority.61 So, concerning the West, it is possible to immediately notice the difference in approach between Europe and the United States.

## Conclusions.

We have tried to describe the phenomenon of digital surveillance by

57 Garante per la Protezione dei Dati Personali, *Regolamento Generale sulla Protezione dei dati* (*General Data Protection Regulation*) – GDPR (May 23rd, 2013). The pdf of the italian version of the Regulation is available at <https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Consideran-do+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018.pdf/1bd9bde0-d074-4ca8-b37d-82a3478fd5d3?version=1.9> accessed 01 February 2022.
58 See ibid art. 17.
59 See ibid art. 7.
60 See ibid art. 83.
61 See ibid art. 77.

analyzing its ethical perspectives and anthropological and political repercussions. First, it must be clear that surveillance capitalism was intentionally conceived in a specific historical period, 'invented by a particular group of people, in a specific place and time. It has been neither a consequence made inevitable by the development of digital technology nor the only possible expression of information capitalism';62 as we have seen in the introductory part of this study, the ideal assumptions underlying the digital revolution were quite different. The biggest mistake that the inhabitants of the digital world can make is to give up because of inurement, by believing in the rhetoric of inevitability and by declaring themselves willing to assign rights: a fair and sustainable digital future can and must be demanded.

However, theorizing an act of rebellion understood as *resistance from below* appears unreasonable because it would concretely result in the indiscriminate rejection of digital tools. This path does not seem feasible (also in light of the ongoing digitalization of public administration). Furthermore, it would also not be fair for people to be forced to renounce the advantages offered by technology, which are objectively evident. So, a first precaution that users could and should adopt to protect themselves is the use of data encryption systems. Nevertheless, the decisive answer to the data protection problem should first and foremost come *from the top*. In the previous paragraph, we have seen how decisive a constant response from the Legislator is, who, due to the extreme rapidity of technological evolution, must – or should – always be ready to reformulate the rules issued by taking into consideration the possible emergence of new rights to be protected. Many place their hopes in the GDPR of the European Union, which, with the procedural changes introduced and the sanctions envisaged, represents a significant achievement. Only over time will it be possible to pass judgment on its effectiveness and say whether it will be able to restore a division of knowledge in line with the values of a democratic society.

62 See S Zuboff, *Il capitalismo della sorveglianza*, 96 (translation mine).