

Ethics and big data: Breaking free from the digital spell

Jean-Baptiste Soufron,
Attorney, FWPA Avocats

Abstract:

Digital technology and big data are not the cure-all claimed by Silicon Valley. They also cause much harm, or even exacerbate the problems and defects of our societies. To regulate big data, a European ethics with respect for individuals and for democratic institutions must oppose the ethics of the Far West.

The entry of individuals into a big data society has been achieved owing to two major misunderstandings. The first is that the digital revolution would primarily be technological and social; and the second, that the technology is neutral, nothing other than a set of tools with consequences that entirely depend on what users want.¹

However digital technology does not have the objective of changing society. To be convinced, we need but remember the titles of Vannevar Bush's seminal article in 1944 "How we may think" and of Norbert Wiener's foundational book in 1950 *The Human Use of Human Beings*. In 1968, Douglas Engelbart presented most of his projects at the Augmentation Research Center. No doubt about it: what is to be changed is human beings. Humans are to be endowed with new capacities via ever lighter devices with ever more connections. From this perspective, the social revolution set off by digital technology is just a consequence of the efforts to create *homo numericus* — a being integrated in a set of cybernetic feedback loops where individual choices are limited, rationalized, controlled.

Whatever the reality (limited to say the least) of its accomplishments, this transhumanism (not to say eugenics) lies at the core of the ethical problems stemming from digital technology. In effect, the advent of augmented human beings does not ensue from a merely philosophical vision alone, but also from an industrial and political program in the most concrete sense. For one thing, this program, which literally applies the lessons drawn from information theory (which facilitates the division of thought), is presented as ubiquitous: it seeks to affect the whole population. For another, it is presented as endowed with rationality and a deeper explanatory power than the rest of science: as being transcendent and, of course, omnipotent.

In other words, the ethics of "uberization" does not stop at details. Under the guise of progress and rationality, the ambition is to apply it to everyone, regulate every aspect of people's lives, change social rules and even foster the emergence of a new morals and spirituality, better adapted to this new environment. It thus uproots the individual and undermines the foundation of life in society, in particular the idea going back to John Locke that the legitimacy of common rules is necessarily, in one way or another, grounded on the group's collective consent. It is echoed in the usual protests against the state's ability to accompany individuals so as to enable them to fulfill their potential. According to a recent study from Stanford, top executives in Silicon Valley mainly identify themselves as Democrats who, pursuing leftist objectives, want to make it possible to develop and fulfill individuals, but who refuse to do so by adopting collective means

¹ This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references.

related to labor unions, solidarity, redistribution through taxes or labor law. This ultimately amounts to wanting social justice while deregulating society as much as possible — a meaningless paradox since this program aims to transform individuals in order to automatically institute social justice thanks to an intelligent regulation via the data on their interactions. In the eyes of CEOs in Silicon Valley, if people need the state, a legislature, courts or organizations serving as intermediaries, as protectors and as a staff, the reason is that human beings need to be improved.

From this viewpoint, the digital program is admittedly a failure. In spite of the paternalistic ambitions of the new captains of digital industry, their services turn out to be stokers that stir up violence and fan lies as much as they facilitate communication and dialog.

Two phenomena are concurrent. First of all, individuals are now forced to spend much of their lives in the form of an intermediary, the digital avatar — a cognitive hallucination that fully exposes them to the fires of envy. Instagram, Snapchat and Facebook turn out to be nothing other than the cybernetic application of mimesis theories. Secondly (and logically), individuals are making themselves sick. Although data, now so widespread, manage to reduce distances and facilitate the transmission of knowledge, they do not transform human beings. We have to concede that our cognitive structure is mostly acquired and that accelerating or augmenting it does not necessarily result in a significant improvement of the individual, and even less in social amelioration. Knowing more and better does not mean thinking more and better. The nudge and automation cannot replace morals and work.

In other words, digital technology and big data are leading to massive, permanent standardization. In the economy, this is reflected in the formation of oligopolies of firms in information and communications technology. For individuals, it corresponds to the inability to reckon with exceptions and with creativity. Nothing resembles an e-mail more than another e-mail, a social network feed more than another social network feed, a like more than another like.

This is not inevitable, of course. The digital landscape has already proven that it can accommodate a degree of humanity. Despite their standardized appearance, the contents of Wikipedia pages reveal their authors' passions and weaknesses. Blogs, curious and brilliant, proliferate, harboring a limitless wealth of information. From Deviantart to Youtube, many websites are havens of creativity for would-be artists who would never have found as easily a venue for expressing themselves elsewhere.

But all this makes the problem more urgent, since there is no recognition of it. When listening to the positions voiced, there is no alternative. By forming an alliance with the sweeping movement of globalization and assuming (at least superficially) the libertarian theories of the Chicago school, the data industry has adopted its own version of the "shock doctrine". It administers it with enthusiasm to each nation-state that asks it for it. For each problem, its solution. For each solution, its data. For each piece of data, a business model. The mere fact of objecting to the systematic dogma of dataism now seems preposterous, since the technology is said to have no other meanings than those that its users want to assign it. However this technology is not neutral, even less so when, as in data technology, it so closely concerns the cognitive operations of human beings.

The founding myth of Silicon Valley makes — to a large degree wrongly so — the impression that the tools we are now using have been invented and developed by private entrepreneurs representing both the American dream and the scientific ideal of a nation turned toward progress. But as Alexander Klimburg clearly explained in his recent article "The darkening Web", we must keep in mind that the military has played an important role in developing the data industry: our lives on line would not be possible without the commercialization of military innovations. The US Defense Advanced Research Projects Agency (DARPA) sponsored the R&D at the origin of: the Internet, the graphic interfaces whereby we interact with our machines, the many tools used by artificial intelligence and by voice recognition technology, and even the high performance polymers needed for the screens of our mobile telephones.

The army is also actively financing this technology. Receiving \$2.5 billion per year, 97% of this sum from security agencies, the Small Business Innovation Research (SBIR) program is the leading source of funding for firms. More importantly, it serves as a government “seal of approval” for private investors. It also provides incentives for entrepreneurship since it is one of the very few sources of finance that do not require equity in exchange for the funds delivered. As an example for showing how this question affects all firms in this business sector, consult Mariana Mazzucato’s remarkable study on Apple in *The Entrepreneurial State*. Although it has spent less than any of the other Big Five on R&D, Apple has succeeded by integrating in the elegant, attractive products it sells the technology (*e.g.*, touch screens, facial recognition) financed by the army and intelligence agencies.

Jacques Ellul and Alexandre Grothendieck, the first persons to point to the ethical dead end of digital technology, were also the first to understand that technology has a meaning and thus calls for a sense of responsibility.

Some persons are reacting violently to a technology with a meaning that seems to them intolerable. Google’s buses have been stoned in San Francisco. In 2016 Cantine, a fab lab and business incubator, was set on fire in Nantes. In November 2017 in Grenoble, Casemate, another fab lab, was vandalized and set on fire because it was said to be an organization notorious for its diffusion of digital culture. Worse yet, in April 2018, Nasim Aghdam, an Iranian YouTuber living in the United States, went to the company headquarters and opened fire on employees because the firm was suppressing videos.

This was not the first time that people turned to violence to protest against automation, digital technology and big data. We need but recall the Committee of Liquidation or Subversion of Computers (the aforementioned (CLODO: Comité de Liquidation ou Subversion des Ordinateurs), active in the Toulouse area in France from 1979 to 1983. Its members planted bombs and set fires (CII-Honeybull in 1980, International Computers Limited in 1980, Sperry-Univac in 1983, etc.). These digital terrorists explained to the media that, as workers in the computer field, they were well placed to realize the dangers, past and coming, of information and communications technology. For them, computers were the tool used by the dominant to exploit, order, control and repress. This was not the only case. In West Germany in 1983, a group called Rote Zellen destroyed a center designing the software for Pershing missiles. In 1984, the Belgian Communist Combatant Cells (CCC) planted a bomb that destroyed the headquarters of several firms in Belgium and Germany. In London, a group called Angry Brigade tried to do the same. Similar actions have been carried out in Asia, South America and, of course, the United States.

These acts of violence have often been described as Luddite, but this is completely false since their perpetrators did not feel that digital technology or big data were menacing their jobs. In a rare interview in English to *Processed World* in August 1983, CLODO explained that its acts were neither reactionary nor new. According to it, when we look at the past, we only see slavery and dehumanization, unless we go back to certain so-called primitive societies. Even though we do not all share the same ideas for society, we know that it is stupid to try to go back in time. For CLODO, the problem was that these tools have been perverted from their origin: the army was the most computerized organization, and 94% of civilian computer time was devoted to management and bookkeeping. To make the point clear while using the words of the opponents of digital technology in 1983, the reason microprocessors caused unemployment instead of reducing the time spent working for everyone is that we live in a violent society. In no case is this a reason for destroying microprocessors.

The movie *Wargames* in 1983 helped to separate computer terrorism from violence. With the invention of hackers (a transitional figure for presenting the digital rebellion in a positive light), digital policy, protests and violence no longer seem to take place in a purely virtual world, a gray zone where moral values are distant and blurred. The very choice of names — White Hat (for good hackers) and Black Hat (for bad hackers) — seems to come from *Lord of the Rings* instead of *The Communist Manifesto*. The foundational book by Steven Levy, *Hackers: Heroes of the Computer Revolution*, marked a turning point. Significantly, its title was translated into French as *L’éthique des hackers* [Hackers’ ethics], which clearly suggests how superficial and definitive the

answer to these important questions has been. The ethics of data? The ethics of heros! Swords drawn, charge with bayonets! It is not surprising that the Grenoble group decried such analyses as a flagrant lie.

What is revolutionary or prophetic in an industry based on old-style capitalism, monopolies, microtasks, money, etc? If Uber were really innovative, it would belong to its wage-earners instead of its shareholders. As for the real heros, recall that MIT's responsibility (an institution supposedly a paragon of innovation) came under question in the suicide of Aaron Swartz, a young man mistreated for having tried to hack a database of scientific articles.

Another development of the digital realm was possible, and still is. Let us not forget that the World Wide Web was invented by CERN in 1989 and that the Web, more than the Internet as such, set off a vast wave of innovations.

The starting point in developing an ethics of data seems to be to consider that digital tools have a meaning. We must then admit that the program for transforming individuals does not have a meaning, whether in its most violent, eugenic form or in the form of a mere nudge, its technocratic avatar.

In fact (and this should come as a surprise to no one), digital technology requires strict standards, intellectual as well as moral. Digital technology, yes; the data, yes too; but to do what? And with whom? By default, we risk ending up in a realm where the choice of the data and of the algorithms for processing them reveals the manipulations, or at least underlying biases, of their designers.

Unfortunately for France and Europe, the digital economy, its technology and tools seem to have mainly served to deregulate industry and public services. The French Post Office and Telecommunications, which the public administration used to manage, has mostly been replaced with e-mail and messaging services run by private firms. In France, newspapers, magazines and audiovisual firms used to operate under legal rules laid down in the important acts of law on freedom of the press (1881) and on freedom of communication (1986). Now they are facing competition from private firms that comply only with the very light rules set by the act on confidence in the digital economy (2004).² Beyond this horizon, no clear industrial vision for digital technology and big data is visible in France.

Given the current scandal of Cambridge Analytica, even a pillar as essential to our society as elections has been disrupted by digital technology and big data. Quite clearly, the risk is to see digital capitalism take roots in an anarchocapitalism that pulls down borders, subordinates states and dismantles the protective rules of the three fictive commodities identified by Karl Polanyi: nature, work and money.

Fortunately, the major (powerful) lines of thought on this topic were formulated more than forty years ago in the French act of on informatics and freedoms (1978). They have turned out to be robust, since the EU's recent General Data Protection Regulation is but a prolongation of them. Foreign giants, such as Facebook, have already announced that they will apply the GDPR around the world. Its principles are simple.³ Data are declared to be personal since they enable individuals to define themselves as persons in a virtual environment. By protecting the data, we are directly protecting persons, citizens. To do this, control is the key. Obtaining consent is obligatory. A person must always have access to his/her data, and be able to modify them or oppose having them processed. What is remarkable for a text more than forty years old is that fully automated decisions with legal consequences for individuals are forbidden by principle in legal and, too, administrative or private matters. This text served as the grounds for censoring, in 2017, the APB algorithm for orienting high school graduates' choices of universities for enrollment — an example showing that the law does not have trouble following up on changes related to innovations.

² Texts of French law are available at: <https://www.legifrance.gouv.fr/Droit-francais>.

³ The GDPR (General Data Protection Regulation): "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". Available via: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1478961410763&uri=CELEX:32016R0679>.

In other words, while the Silicon Valley Far West has enabled the United States to develop a data industry, it is the social, personalistic ethics of solidarity in Europe that might manage to regulate this industry. In this respect, the recent proposals made in the Villani report have come at the right time: an audit of artificial intelligence, citizen assessments, research on explicability, courses and training programs in ethics in engineering schools, impact assessments, collective rights, group actions, an observatory on the nonproliferation of autonomous weapons, committees of ethics, etc.⁴

Although these proposals provide operational solutions for public policy, they do not answer the questions raised: by the growing individual entropy generated by the shift toward a data society, by the right to refuse certain technological procedures as a function of their meaning (and not just for reasons of efficiency), by the protection of the weak from the strong and, too, of the weak from the crowd, etc. A first step in this direction would be to restore the principle of democracy, which has been endangered informally by scornful declarations and the power grab by certain leaders in the digital economy. It has also been endangered formally by direct offences as in the large-scale campaigns of manipulation now being orchestrated during each major election in the West. A second step would, for sure, be to rework the immense, still unused, possibilities that, short-circuited by online platforms and the social media, have been a major source of disillusion.

Of course, we must take account of personal (individual and family) issues. It is not normal that the data society entails psychological suffering: the “detachment” in families, ever stronger social pressure, or even violence. It is necessary to learn how to manage our digital avatars so that we do not have to constantly produce data or accept their processing in order to be able to live in society.

Finally, it is necessary to pay attention to the question of meaning. This probably implies a return to fundamental tools, such as authorizing or forbidding algorithms, just like, already in 1978, the French act of law prohibited the collection of data on political opinions or ethnic affiliations. Are all data good to use? Probably not.

⁴ VILLANI C. (2018) *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*, mission parlementaire, March, 242p. Available via: https://fichiers.acteurspublics.com/redac/pdf/2018/2018-03-28_Rapport-Villani.pdf.