Winter January 11, 2016

"Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data.

Antoinette Rouvroy

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 11 January 2016

T-PD-BUR(2015)09REV

BUREAU OF THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS 108]

(T-PD-BUR)

"OF DATA AND MEN"

FUNDAMENTAL RIGHTS AND FREEDOMS IN A WORLD OF BIG DATA

Antoinette Rouvroy*

The views expressed in this report are those of the author and
do not necessarily reflect the official position of the Council of Europe

Directorate General of Human Rights and Rule of Law

* Permanent Research Fellow of the National Fund for Scientific Research at the Research centre Information, Law and Society (CRIDS), University of Namur, Belgium. For his attentive rereading and valuable comments which have informed this paper, I would like to express my sincere gratitude to **Jean-Noël Colin**, Professor at the Faculty of Information Technology at the University of Namur. My thanks also go to **Alessandro Manteloro** for his extremely relevant comments concerning certain aspects of the Part 2 of this report.

Contents

PREFACE

In order to have a clearer picture of the innovations introduced by Big Data-type processing as compared with the processing of personal data covered in particular by the Council of Europe's Convention 108, the first part of this report will focus on describing the *data* covered by the term Big Data, the *processing procedures* of these data and some of the associated *ethical, legal and political issues*.

The decision to deal with both the technical and societal aspects is a result of the realisation that there is an inextricable interdependence between the semiotic, epistemic, ethical and political challenges in the context of Big Data. We shall see, for example, that the statistical practices involved in Big Data-type analyses introduce a new way of sub-contracting to automatic systems the task of ensuring that the categories (of merit, need, desirability) which govern the distribution of resources and opportunities in our society emanate from this digital reality itself rather than their being instituted politically or agreed upon contractually.

Accordingly, having an understanding of the rationality of the algorithmic processes (data mining, machine learning, etc.) is a necessary precondition for any normative reflection on Big Data in terms of the rule of law and fundamental rights and freedoms. Account must be taken of the changes that have taken place in and the considerable diversity of the calculation processes involved in Big Data-type processing.[1]

There are countless applications of the new techniques involved in analysing and exploiting Big Data. The category of applications of interest to us here is the one which employs the modelling of human behaviour and predispositions for various purposes on the basis of data coming from individuals and the contexts in which they live, or which are produced automatically.[2]

[1] Here, we need in particular to identify as precisely as possible the processes associated with data mining, machine learning, social network analysis, predictive analytics, "sensemaking", natural language processing, visualisation, etc. insofar as these processes pose specific problems. In this report, however, we focus in particular on data mining and machine learning, while bearing in mind that other Big Data-type processing procedures have marginally specific implications in terms of data protection and protection of privacy.

[2] *Excursus*: We could also have opted not to differentiate between human and non-human since the "units" of Big Data are not individuals or objects, but data – the concepts of individuals, subjects, persons, or even groups or communities are by definition, one might say, excluded from the Big Data universe – and since the Big Data phenomenon and the new data correlation methods cause the digitised reality to cut itself off, leaving "on the outside", as it were, bodies, physical objects and any "thing" having a rigid "form". It is not the effects of anthropocentrism that cause us to focus more particularly on the modelling of human behaviour and predispositions rather than on the modelling of other possible events in the world, but because humans, more no doubt than other living creatures and certainly more than inanimate things, generally react, occasionally in advance, to the descriptions and entries concerning them to either fit in with them or deviate from them and because, as they have the ability to speak, they have this capacity for contrariness, for response, for transcending any label, characterisation or profiling attached to them: humans "respond" as the humans that they are, whereas the other animals are unable to respond when they are named, or designated unilaterally (see in this connection Jacques Derrida, "The animal that therefore I am", in *The Autobiographical Animal*, Fordham University Press, 2008), even though it cannot be absolutely ruled out, although it is unlikely, that amongst themselves in their animal language they label us with a name, to which we ourselves are unable to respond. Although the concepts of human, non-human or even inhuman have no place in algorithmic rationality, nevertheless, among living creatures, human beings have a particular ability to withstand the process of categorisation or labelling and to remain in a relative indeterminate state. It is precisely this indeterminate state, in which the underlying indecidability in the field of human affairs takes root, that the algorithmic

This report is divided into two parts. Part 1 (Big Data: technical, epistemic and societal challenges) is an attempt to identify the radical innovation introduced by the world of Big Data and the associated societal challenges.

Part 2 (**The Council of Europe's Convention 108 in the Big Data age**) strives, in accordance with the terms of reference we were given, to identify how the personal data protection system can help find responses to some or all of these societal challenges and offer some avenues to explore with regard to the possible revision of the Convention to take account of the Big Data phenomenon. Given the complexity of the challenges involved, which makes it all the more difficult to uncover and present them (we would need to be able to write in three dimensions at least) we have opted for a number of solutions intended to make things easier for the reader. In order to differentiate between them and other considerations, the specific proposals we are putting forward are presented in boxes. Whenever we refer, in bold type but with no further precision, to numbered articles, we are referring to the articles in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, in the amended version resulting from the work of the Convention 108 Consultative Committee.[3]

Insofar as the Big Data phenomenon is likely to concern virtually all sectors of activity and government, it will of course be impossible to draw up an exhaustive list of all the current and future challenges that it poses. At most, this report will be able to provide a few examples highlighting the relevant issues from the point of view of data protection and, more generally, the protection of fundamental rights and freedoms.

optimisation of decisions seeks to overcome in order to bring about greater efficiency, greater operationality to the point where we could become obliged, exposed as we are to forms of categorisation to which we are unable to respond, to ultimately find common cause with animals.

[3] Draft protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

1 BIG DATA: DESCRIPTION, TECHNICAL, EPISTEMIC AND SOCIETAL ISSUES

1.1. Volume

It is estimated that the digital universe today is made up of more than 1,200 billion billion bytes,[4] 90% of which would appear to have been produced in the last two years. This number, which doubles every two years, will need to be multiplied tenfold by the year 2020, reaching a total of 44 zettabytes,[5] or 44 trillion de gigabytes.[6]

The translation or rather transcription by computer systems of the physical world and its inhabitants in the form of metabolisable data is no longer limited or fundamentally restrained by technical or economic inaccessibility. While the collection, transport and storage of data clearly have a direct cost,[7] this cost decreases in accordance with Moore's law (the doubling of the data recording capacity on a silicon chip every 18 months,[8] thereby increasing processing capacity, and therefore efficiency by making it possible, thanks to the multiplication of transistors, to carry out a large number of complex operations) and Nielsen's law (connection speed doubles every 21 months).[9] Reference may also be made to Kryder's law, which in 2005 predicted that magnetic disk storage density would double every 13 months. If we add to this the appearance of new storage formats such as SSD, it becomes clear that we are able to store an increasing amount of data and access them increasingly more quickly. Consequently, what we are seeing is an exponential increase in processing capacity (Moore), storage capacity (Kryder) and communication capacity (Nielsen).

The exponential increase in Big Data is a result of the retention by default not only of directly useful data (the usefulness of which[10] is defined by the actual use for a given purpose[11]), but also of the data whose usefulness has expired (and which are no longer necessary for that purpose), and those data which are merely of potential utility. It is the quantity (or volume) much more than the quality of data which can give rise to an unexpected usefulness of all sorts of data, including those which on the face of it are the least meaningful, operating as pure signals, individually carrying very little information (referred to occasionally as "weak signals") or indeed meaningless, derived from the connected world.[12]

---

[4] A byte is the digital unit required to encode a single character

[5] A zettabyte equates to 1,000,000,000,000,000,000,000 bytes.

[6] Turner V., Gantz J. F., Reinsel D., Minton S., "The digital universe of opportunities: rich data and the increasing value of the Internet of things", April 2014, IDC #IDC_1672, EMC study, http://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf.

[7] We shall not discuss here the indirect costs for the environment and health of the development of digital technologies.

[8] Or every 24 months, depending on the version consulted. Moore's law logically comes up against the physical limits of miniaturisation.

[9] http://www.nngroup.com/articles/law-of-bandwidth/

[10] See, in particular, the report by the OECD's Working Party on the Information Economy and the Working Party on Information Security and Privacy, *Exploring the economics of personal data: a survey of methodologies for measuring monetary value,* 2 April 2013, DSTI/ICCP/IE/REG(2011)2/FINAL, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/IE/REG(2011)2/FINAL&docLanguage=EN

[11] For a very clear description of the phenomenon, see Delort P., *Le Big Data,* PUF, Collection "Que sais-je?", 2015.

[12] Ibid.

Accordingly, the usefulness of each data item depends on the quantity of the other data with which it may be correlated, more than the density of information it carries. Even data carrying very little information (anonymous data which, individually, are absolutely mundane and meaningless) become more useful the more numerous they are.[13]

In the Big Data universe, it is therefore perhaps not going too far to think that by means of a network effect,[14] the potential value of each piece of data increases to the point where it may exceed its current value depending on the quantity of data collected. According to certain estimates reported by the European Commission, the increased revenue generated each year by the personal data of European citizens has the potential to grow to nearly €1 trillion by 2020.[15] This usefulness or value of data is clearly neither visible nor accessible to individuals who merely act as temporary, often mundane, "infra-individual" data aggregates exploitable en masse on an industrial scale. There are, accordingly, two conflicting approaches concerning the general philosophy of data protection instruments and the "status" of personal data. On the one hand, there is the "law and economics" approach, which is also that of those advocating a personal data "market", which tends to regard personal data as marketable "goods", given that they are in fact marketed (by companies, data brokers, etc.), and to allow individuals to negotiate the transmission of "their" data for financial remuneration, and on the other hand, the approach which addresses personal data more from the point of view of the power they confer on those controlling them and strives to prevent excessive disparities in information and power between those who process the data and the individuals themselves. Quite clearly, it is this second approach that prevails in Europe.

1.2. Variety

A further feature of Big Data is their variety. Apart from the variety of formats (text, images, sounds, geo-location, mobility data, etc.), the data likely to be simultaneously processed in Big Data-type analyses come from a multitude of sources and may be structured or unstructured.[16]

Hard data are produced by institutions and public administrative authorities (data produced during censuses, property registers, complaints and court decisions, balance sheets and bankruptcies, data relating to driving licences, electoral rolls, registers of

[13] It is this, moreover, that gives GAFA, the four Internet giants (Google, Amazon, Facebook, Apple) undeniable advantages in the Big Data economy (even though Apple has so far refused to enter into the data business). These data clearly have a monetisable value: the socio-demographic and psychographic data (lifestyles, beliefs, values, personality) held by a social network such as Facebook for example on all its users have a huge economic value given the prospects they offer for a very precise segmentation of its client base, or for targeted advertising

[14] A network effect is one whereby the actual value – of a technique or product, for example – depends on the number of its users. Transposed into the Big Data context, the network effect theory would produce the following: the actual value of a data item will depend on the quantity of other data collected with which it could be aggregated.

[15] European Commission, "The EU Data Protection Reform and Big Data – Factsheet", April 2015, http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf

[16] "Structured data are data all of whose possible values are determined and known in advance. For example, in a database containing the results of an opinion poll, the age and socio-professional category of the people surveyed are structured data because the age brackets and the list of possible socio-professional categories are determined beforehand. Freely expressed responses to open questions are unstructured data because each of these replies is potentially different and impossible to categorise in advance. In a client e-mail database, the author and date are structured data, but the message body is unstructured." (*Didier Bourigault,* "L'avènement du Big Data révèle la valeur des données non structurées", *http://www.synomia.fr/fr/vision-et-techno/synomia-menu-la-data-non-structuree*)

births, marriages and deaths, licences of all kinds, etc. The digitisation of public documents is not without impact on the private lives of citizens. Public documents which were not formally part of private life in archived paper format were, in practice, covered by a sort of practical opacity, whereas once digitised their public exposure becomes significantly more probable. This is one reason why the opening up of public data must involve data anonymisation processes.

Today, when we work, consume or travel we inevitably "produce" data.[17] We classify as soft data the data produced by individuals, either intentionally via blogs, social networks and discussion forums, or unintentionally inasmuch as an increasing proportion of their activities, interactions, online and offline movements leave digital "footprints" which are often collected by default by mechanisms to monitor online movements, CCTV, GPS tracking, traffic flow monitoring, satellite imagery, recording of banking transactions, etc. and which are stored for various purposes, rarely made clear at the time of collection. Although the digitisation of the world does not meet with any significant reluctance from individuals, this is because it seems to be the inevitable, indissociable and necessary cost of a multitude of new services, new functionalities of digital devices, the ability to engage in social interaction via digital processes, the enrichment of the perceptive field of individuals through personalised, dynamic and contextualised information, new relationships with oneself, one's health, one's productivity, a personal self-monitoring and prevention relationship via "quantified self" and "connected health" digital devices, and also a certain predilection for surveillance when it extends the individual's capacity to monitor family and friends.[18]

To all this are added metadata which – in the more general sense – are "data about data", i.e. data, at times generated automatically by the computer systems themselves, which make it possible to describe and structure other data, regardless of their content. Metadata may, for example, be data about the location of data, about the type of data available, about the source of the data, etc.[19] Examples are the traffic data referred to in Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, which can include data on the routing, duration, time or volume of a communication, the protocol used, the location of the terminal equipment of the sender or recipient, the network on which the communication originates or terminates, or the beginning, end or duration of a connection. They may also hold details of the format in which the communication is conveyed by the network. They also include location data which, as defined in this same Directive may refer "to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the

[17] Sadin E., *Surveillance globale. Enquête sur les nouvelles formes de contrôle.* Climats/Flammarion, 2009

[18] *Excursus*: For example, it can happen – without this giving rise to any debate – that parents of children attending nursery school ask the teacher (who is happy to oblige) to take photos of their children throughout the day and post them on a dedicated Facebook page so that they can, at any time of the day, consult them via their smartphone. Digital apparently fun and congenial social practices dissolve the walls of the school fostering the ominpresence of parents, and make the trust that is due to the teacher conditional on the possibility of monitoring at any time the state of well-being of their children. Over and above the issues of protection of privacy and personal data, we should not overlook the reconfiguration of social space brought about by this new porosity of contexts which previously were less permeable to digital flows. In the education field, insurance sector, employment or even romantic relationships, the requirement for absolute transparency, fine-grained and continuous control replaces the asymmetries of information which result from the differences in roles, positions, situations and intentions between individuals or which are justified by equity or the requirement of solidarity (in insurance). This obsession for transparency, for direct and immediate access to data, dispensing with an account, report or testimony, is paradoxically combined with a lack of interest in understanding, controlling and evaluating (in terms of legitimacy, equity and justice) the (automated) categorisation processes emerging from the processing of these data.

[19] Adriaans P. and Zantinge D., *Data mining*, Harlow, England, Addison Wesley Longman, 1996.

location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded." More specifically, metadata also includes the data on which a data item was produced or recorded, the GPS co-ordinates of the place where a photograph was taken, the duration of a telephone call, etc. All these metadata were covered by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, declared invalid by the CJEU on 8 April 2014.[20] The fact that they no longer have to be kept in order, if necessary, to be made available to the public authorities, does not mean of course that they may not eventually be used, in particular for the identification of individuals or for profiling purposes.

Lastly, an increasing proportion of digital data comes from what is now referred to as the *Internet of Things:*[21] the networking of "smart" devices able to communicate with each other and therefore themselves to produce huge amounts of data.[22] These networked devices emit information on the movements, activities, performance, energy consumption, lifestyles etc. of their users.[23]

All these data are either collected first hand by administrations or companies, or acquired at a hefty cost from other administrations or companies or from data brokers (also called information brokers, information resellers, information aggregators or information solutions providers) who make a living out of collecting, aggregating and providing the means to analyse and exploit massive amounts of data.[24] As individuals have no direct interaction with these data brokers, they have no way of knowing the extent or nature of the information collected and sold for a multitude of reasons including fraud prevention, marketing and credit scoring.

Being able to process simultaneously these different types of data is a constant challenge for Big Data practitioners. While the costs of collecting, transporting and storing data are constantly falling, the same is not true for the cost of analysing these data. In order to be valuable or useful – as "raw data" in themselves have no value – the data must be processed. They must be extracted from their original source, cleaned up, standardised and validated before they can actually be exploited. Transforming raw data (in various formats) into operational "knowledge" requires substantial investment. The economic question is therefore, each time, to assess whether the value of the results of the analysis based on Big Data is likely to outweigh the cost.

1.3. Velocity

A third feature of Big Data is the speed with which they are accumulated in "real time".

---

[20] Judgment of 8 April 2014 in Joined Cases C-293/12 and C-594/12.

[21] In 2020, it is anticipated that 50 billion devices will be connected to the Internet (The Internet of Things. How the next evolution of the Internet is changing everything, Cisco White Paper, 2011, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf)

[22] http://france.emc.com/leadership/digital-universe/index.htm

[23] cf. Opinion 8/2014 on Recent Developments on the Internet of Things: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[24] See, in particular, *Data Brokers. A Look at the Canadian and American Landscape*, Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada, 2014, https://www.priv.gc.ca/information/research-recherche/2014/db_201409_e.pdf; *Data brokers. A Call for Transparency and Accountability*, Federal Trade Commission (US), May 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Never before have data sets been able to be extended so flexibly. This also means that the usefulness, "significance" and value of data evolve in real time, in line with the inflow of new data.

It is not only the speed with which data are accumulated but also the speed with which they are processed which bypass and deactivate the processes of human perception and understanding, and the processes of proclaiming motivations. For example, the target of devices for the detection, classification and predictive assessment of human behaviour and propensities (whether used in the field of security, combating terrorism or marketing) is not an individual's statement of intent or the first stages of carrying out those intentions, but the processes preceding them, often at a pre-conscious stage. (In the part of the report dealing with digital surveillance and predictive analysis, we shall look at the challenges inherent in these new capabilities in terms of informational self-determination, of the right to the protection of privacy insofar as this protects individuals against excessive intrusion in their personality development processes, and of safeguards against direct and indirect discrimination).

One might think that all this is science fiction. Not at all. If we are to believe Eric Schmidt, Google's CEO, technology will soon become so effective that it will become very difficult for people to see or consume something that has not in some sense been tailored for them.[25] In the marketing field, ultimately the aim is not so much to adapt supply to individuals' impulsive or spontaneous desires (insofar as such exist) but rather to adapt a person's wishes to what is on offer, by adapting sales strategies (the time when advertising is sent out, the way the product is presented, setting the price, etc.), the design of the interface (so as to inspire trust and nurture a desire to consume) to each individual's instinctive drive profile.[26] In this way, we are perhaps moving from an intention-based economy to an instinct-driven economy. The online bookstore Amazon recently patented software enabling it to ship merchandise to its clients even before they had actually placed an order.[27] The call centres of certain companies, rather than assessing candidates based on their CV and a recruitment interview, use workforce optimisation software (the term used by the recruitment industry based on modelling produced by Big-Data type processing)[28] which detects, out of all the information available particularly on social networks, not directly whether candidates have the required qualities for the job, but whether they match certain data points, which on the face of it are unrelated to the qualities the post or job will require (such as being signed up to two social networks rather than three or just one) but which are statistically predictive of, amongst others, good performance or the ability to cope with the demands of the vacant position.[29]

These "performance prediction" tools for purchasing intentions (which is also a means of bypassing the process of transforming impulse into desire or articulable intention), or workforce optimisation based on the predictive detection of future performance derived from indicators produced automatically from Big Data-type analyses (which also signifies a sharp decline in the value of experience and individual merit on the labour market) raise countless questions. Are the prediction of intentions and the new

[25] http://online.wsj.com/news/articles/SB10001424052748704901104575423294099527212
[26] See Calo R., "Digital Market Manipulation", *George Washington Law Review*, 82, 2014.
[27] Bensinger G., "Amazon Wants to Ship Your Package Before You Buy It", *The Wall Street Journal*, 17 January 2014
[28] See, for example, *Evolv*, a company offering this type of workforce optimisation software: http://www.cornerstoneondemand.com/evolv
[29] Guillaud H., "L'emploi à l'épreuve des algorithmes", *InternetActu*, 3 May 2013, http://www.internetactu.net/2013/05/03/lemploi-a-lepreuve-des-algorithmes/

possibilities of pre-emptive action based on the detection of intentions compatible with the pursuit of the self-determination of individuals? As opposed to the utopia or rather dystopia of a society freed from the burdening experience of the incalculability of events and behaviours, as opposed to the apparent temptation of a society in which deciding required nothing other than the scrupulous application of automatic recommendations, and as opposed to the possibly seductive prospect of a world in which decisions cease to bear the stigmata of subjective involvement, should we not take the view that the ability to articulate for ourselves and tell others about our intentions and motivations is a key factor of self-determination? How can we ascertain how fair these practices are? Is workforce optimisation, based on digital profiling compatible with the principle of equality and non-discrimination?

1.4. Reliability without truth: new processing logics

Above all, therefore, the terms Big Data refers to the crossing of a threshold of data quantity, complexity, and proliferation speed, beyond which we have no choice but to automate and speed up (in order to cope with the constant and ultra-rapid increase in volumes of data) the processes for transforming digital data into operational information.[30] The term Big Data therefore refers not only to the huge volumes of complex, rapidly accumulated digital data, but also to all the new software techniques (data mining, machine learning, social network analysis, predictive analytics, "sense making", natural language processing, visualisation, etc.) without which the data would tell us nothing, and which presuppose, in turn, the use of immense storage and processing capacity. As this power cannot be provided by a single computer, no matter how powerful, the solution is to opt for the parallelisation of processing and data based on the simultaneous use of a large number of servers configured in clusters on which data are distributed[31] and which work together using distributed processing models[32] to detect subtle relationships, which would otherwise remain imperceptible, among very diverse data collected in various contexts.

Of course, the reliability of the "knowledge" resulting from Big Data analyses is anything but certain:

First, it is not because they appear to be "collected by themselves" that the data are accurate and relevant. The quality and relevance of data depend to a very large extent on the quality and location of the sensors, and on the extent to which the relevant information is able to be digitised. In addition, the algorithmic modelling, rather than offsetting human bias and prejudice, can merely record and "naturalise" them (by transforming them into "data"), making the bias they may contain imperceptible and unchallengeable.

- *An "inherent rationality"*

Rather than subsuming data in pre-established categories (such as statistical categories, requiring a potentially lengthy conventional process in order to be set up), Big Data-type processing produces "categories" from the huge volume of data themselves, virtually in real time. These algorithmic "categories", also termed models or profiles (when referring to human behaviour) are dynamic patterns (the term data visualisation is also used) formed from correlations observed not in the physical world

[30] Weinberger D., *Too big to know: Rethinking knowledge now that the facts aren't the facts, Experts are everywhere, and the smartest person in the room is the room*, New York, Basis Books, 2012.
[31] For example, the Hadoop software.
[32] For example, MapReduce.

but among the digital data collected in diverse contexts, independently of any causal explanation. In other words, unlike conventional statistical processing, in which statistical hypotheses or categories precede and govern the collection of data, in Big Data-type processing, the exact opposite occurs: *data collection and processing come first and give rise to hypotheses or categories from among the mass of data*.

Consequently, the algorithmic categories, "models" or profiles have an aura of objectivity which is much greater than that of statistical categories. As Alain Desrosières[33] explained very clearly, traditional statistics – given that it is necessary to agree on the criteria making disparate events, performances and phenomena commensurable and therefore able to be placed in the same statistical category – are the product of social conventions (which he calls conventions of equivalence), making it possible to compare what in their absence would be incomparable), and therefore are presented not as objectively reflecting reality but as representations of the world with at most the aim of being neutral. The statistical processing inherent in Big Data analysis seeks to dispense with all conventional, political and ideological operations, and with all discussions on the categories through which we perceive the world since the categories produced emerge "spontaneously", thanks to algorithms able to detect statistically meaningful correlations.

Whereas, when they serve as references for public debate, "traditional" statistics may always be open to question (have sufficient data been taken into account? Have too many data been considered?), algorithmic modelling (patterns or profiles) would appear, in principle, to escape any form of challenge since these models are neither produced nor constructed but, in contrast, appear to derive directly from the digitised world, with the data clusters having been selected on no other basis than their technical compatibility with the Big Data-type analysis systems.

The extension (postulated by the Big Data ideology) of both the statistical base and the digital reality is an incorporation of what traditional statistical practices could not deal with: points that were too far removed from the mean (which could give rise to claims that statistics were of use only for large numbers, not for individual cases) and results that did not fit into any category (with regard to statistical objects from conventional sources it was always possible to argue that they had failed to take into account enough data or had taken account of too many). All these were excluded areas for a statistical approach which sought to represent the world in certain of its aspects and not to replace it. The incomplete and selective nature of traditional statistics vis-à-vis the constituent elements of the world should not be understood as a "weakness" of statistics but as an essential precondition for "statistical thinking".

In the Big Data world, the aura of objectivity and exhaustivity of digital data, and the widespread idea that "governing by data" would be a means of governing "objectively", the perception being that the meaning produced by the analysis of data, conceived as pure signals coming directly from the world in real time, would no longer be constructed

[33] In an interview with Christian Mouhanna, Alain Desrosières explained that "Statistics are the product of social conventions. Rather than ask whether they objectively reflect reality, it is more productive to see them as just one of the representations of the world and to question the objectification processes. Rather than 'neutrality', we could refer to the 'aim of neutrality' on the part of professional statisticians, just as Jean Ricœur spoke of the 'aim of describing reality' with regard to the work of historians. Statistics are not neutral in principle. Only by reconstituting the way statistics are produced and used is it possible to evaluate their real scope. The words 'objectivity' and 'neutrality' implicitly refer to the metrology of the natural sciences, whereas economic and social statistics can be more usefully compared with law and political sciences, insofar as their conventions are social products governed by metarules, which are also conventional." ("Interview with Alain Desrosières" *Sociologies pratiques* 1/2011 (No. 22), p. 15-18.: www.cairn.info/revue-sociologies-pratiques-2011-1-page-15.htm.)

socially, politically and culturally but would be the equivalent of an automatic unveiling, beyond language, of the world by itself, uninterpreted, unsymbolised, unrepresented and independent of any ideological perspective, is probably one of the epistemic reasons for people's acceptance or tolerance of the digitisation of the world. The Big Data ideology is the utopia of immediate access to the world, outside the constraints of language. The digitisation of the world offers a radical response to the crisis of "representativeness": there would no longer be anything to represent, and nothing left to challenge, since the data inherently "speak for themselves".[34] Consequently, the huge excitement over Big Data would appear to be leading us towards a sort of loss of distinction between the world and its digital representations, and a loss of distinction also between technology and culture – and therefore towards a quantitative depoliticisation.

However, inherency is not synonymous with truth. Nevertheless, the validation criteria used for algorithmic modelling are in no way comparable to scientific validation criteria. It is, for example, almost impossible to replicate the algorithmic operations in a context in which the data clusters in question are constantly expanding. Moreover, the aim of this modelling, which can be said to be produced at the level of the digital world rather than in relation to the physical world, is not at all to describe the "truth" but simply to be "operational". Validity is no longer a question of "truth" but of "reliability" – "reliability without truth", wrote Eric Winsberg,[35] a reputedly even greater reliability since the processes are automatic and avoid human intervention – and the obviation of the search for truth, and for historicity and causality, is precisely one of the driving forces of the new algorithmic rationality. This is the idea of the "black box": we know what goes in on one side and we see what comes out the other, but we do not know what goes on between the two. The fact that the world as it actually occurs does not comply with the algorithmically produced model, the algorithmic reality – i.e. when what appears in the world belies the profiling that had been carried out – is in no way a failure: these concepts of failure are meaningless in a digital reality in which any deviation from a statistical model is immediately assimilated into the statistical base in order to refine the model. This is the very principle of machine learning, supervised or unsupervised.

Learning is said to be "supervised" when the algorithm is trained on learning data provided by the human supervisor, which contain both the data and the anticipated results (for example: medical parameters and diagnoses) to enable it to function independently on sets of data for which the results are unknown, in a generalisation process. Supervision serves to validate and (re)calibrate the model selected by the algorithm (which it will have identified as the "correct" solution) to assist the system in focusing its modelling in the desired direction.

Learning is said to be "unsupervised" or bottom-up when the system is given no previous model to learn from. It is given no set of training data and no "correct solution" to serve as a model. The algorithm is left to analyse the data and identify correlations between them in the hope of showing up underlying models. One example of such an algorithm is that of clustering, which can identify 'similar' individuals within a population group.

The self-learning algorithm is capable of producing unexpected solutions, radically new

[34] However, we know that data are never just "data" but are invariably the result of a sophisticated process of transcribing reality in metabolisable form by computers.
[35] Winsberg E., "Models of success versus the success of models: reliability without truth", *Synthese,* September 2006, Volume 152, Issue 1, pp. 1-19

patterns or models, imperceptible to our ordinary senses and, in particular to the human eye (cf. below, p. 35). Of course, the algorithm must be trained to eliminate spurious or irrelevant correlations.[36] Furthermore, the fact that there are no hypotheses or models governing the work of the algorithm does not mean that there are no assumptions, in particular with regard to the characteristics of the environment in which the algorithm is working. For example, an algorithm operating on the assumption of a stable, unchanging environment will be unable to deal with any changes to that environment, which would result in its producing incorrect, irrelevant or ineffective solutions. In particular, this algorithm would be unable to predict future behaviours. However, faith in the objectivity, effectiveness and operationality of algorithmic predictions often, among those who adopt them for various purposes (preventing insecurity and terrorism, detection of propensities to fraud, prediction of purchasing behaviours, optimisation of human resources, etc.), overrides the process of critical evaluation of what is more often than not presented as a recommendation or automated decision support system. Insofar as these automatic facilities are purchased and put into operation specifically to speed up and objectivise decision-making processes, their "predictions" are almost systematically turned into actions and interventions which, in turn, modify the state of affairs in a way which makes it no longer possible to identify, counterfactually, what would have happened if the automatic recommendation had not been acted upon. Accordingly, prediction does not merely describe the future, it transforms it so that it becomes extremely difficult – in the absence of ground truths – to test the self-learning algorithms to evaluate effectively their epistemological validity.

Ultimately, therefore, one could say that the "success" of an algorithm is measured less in terms of the "truth" of the models it produces than in terms of the speed with which operational information is achieved at minimum cost.[37] The rationale is one of output and optimisation, not at all of truth, validity and even less so legitimacy.

The fact that the criteria of differentiation between individuals cannot be criticised[38] means, *both for individuals who are the subject of profiling and those who use this profiling to take decisions affecting individuals,* a lessening of responsibility – ever fewer opportunities to "respond" – ranging from exemption from giving reasons for one's acts or decisions to the impossibility to do so. Faced with this, there are two possible solutions: the first – based on the assumption of a perfect superimposition between objectivity/truth and justice – is to ensure, through technical means, the objectivity and unbiased nature of algorithmic modelling (*algorithm auditing etc.*).[39] The second – based on the assumption of the irreducibility of justice to mere objectivity –

[36] Hildebrandt M., *Smart Technologies and the End(s) of Law*, Edward Elagar, 2015, p.24.

[37] Karsenty J-P., "Big data (mégadonnées). Une introduction", *Revue du Mauss permanente* (http://www.journaldumauss.net/?Big-Data-megadonnees-Une), 1 April 2015)

[38] Rouvroy A., "The end(s) of critique: data-behaviourism vs. Due process", in Hildebrandt M. and De Vries E. (eds.), *Privacy, Due Process and the Computational Turn.* Routledge, 2012. Available at: http://works.bepress.com/antoinette_rouvroy/44

[39] See, for example, the study by Datta A., Tschantz M.C. and Datta A.,, "Automated Experiments on Ad Privacy Settings: A tale of opacity, choice and discrimination", *Proceedings on Privacy Enhancing Technologies 2015* (1): 92-112 http://www.andrew.cmu.edu/user/dnupam/dtd-pets15.pdf. In this study, the authors make the case that the result of interaction between users' behaviour, declaration of gender in their "Ad Settings" preferences and Google advertising personalisation software was that those who had identified themselves as male were much more likely than female respondents to receive advertisements for highly paid professions (advertisements for executive coaching services).

consists of requiring the possibility of challenging decisions[40] impacting individuals, whether or not these decisions are based on the automatic processing of data. Here, it is no longer a question of being accountable merely for the objectivity of the algorithmic processes but also for the just, equitable and legitimate nature of the decisions taken in accordance with these processes. In other words, we need to put the focus once again on "non-necessity" – without which there can be no decision (true decision-making presupposes that no solution is imposed out of necessity) but simply obedience or conformism – to make room for what is incalculable and undecidable by calculation. We shall attempt (cf. 2.6 below) to identify how, for example, the reversal of the burden of proof in cases of suspected indirect discrimination caused by automatic recommendations, or the introduction of a general principle of the ability to challenge decisions taken on the basis of automated processing (algorithm audit, etc.) could help restore individuals' *capacity to be accountable and state for themselves* what had prompted them to act in such a way or take the decisions they had made. This capacity to express – with all the potential for fabrication that this entails – is at the heart of the concept of legal subjectivity, and perhaps more so than the capacity for understanding and volition, traditionally regarded as occupying the centre of gravity of any subject of law.

- *Personalisation or individualisation rather than categorisation.*

A further aspect of Big Data-type processing is linked to the (relative) non-selectivity in the collection and storage of data: whereas traditional statistical practices eliminate from the data cluster all the data points which are too far from the mean or the "most likely" to give rise to errors and confusion, Big Data-type processing implies, in contrast, taking "everything" into account, including what is most exceptional, furthest away from the large numbers, with these anomalies not even being related to any mean (the very concept of "mean" losing all relevance). This is what makes "personalisation" processes possible, i.e. differentiation in line with ever more numerous and precise "profiles" (of potential criminals or fraudsters, consumers, users, etc.) and security, commercial, educational, medical interactions, etc. This means in practice that whereas in the context of traditional statistical processing, it was possible to claim that statistics applied to large numbers but not to individual cases, the Big Data approach seeks to ensure the relevance of "categories" for the most exceptional cases, or in simpler terms seeks to replace categorisation by personalisation or individualisation.

In the actuarial and insurance world, the burden corresponding to the irreducible cost of radical uncertainty, deriving from the fact that one can never be certain that everything that is possible or probable will actually occur, is borne by various forms of sharing, i.e. the collective covering of the risk.[41]

[40] On this subject, see Citron D.K., Pasquale F., "The Scored Society: Due Process for Automated Predictions", *Washington Law Review*, 2014, Vol. 89, 2014, p. 1-; U of Maryland Legal Studies Research Paper No. 2014-8. Available at SSRN: http://ssrn.com/abstract=2376209

[41] François Ewald, in connection with the calculation of probabilities at the heart of insurance practices, explained that it functioned as "a ruse of reason". The calculation of probabilities is an investigative tool to offset the impossibility of explaining phenomena in physical terms. It is a tool of experimentation through pure reason. It is not only that we do not know the laws governing the phenomena we perceive in their infinite variety and their infinite dispersion, we also do not know their causes. Our lack of understanding is such that, even if we were able to infer certain regularities, we would be unable to determine whether these regularities constituted laws. The paradox of the calculation of probabilities results from the fact that this fundamental lack of understanding cannot be overcome by any knowledge coming from a discovery, and that we will never leave the realm of observation. The whole art of calculation therefore consists of

With the arrival of Big Data (and of phenomena of quantified self), this sharing of the risks tends to give way to a much more individualising approach, attempting – through the composite nature of Big Data-type analyses – to determine for each person individually, his or her "individual risks" and "real costs", a way of individualising the risk and, at the same time, unravelling the mechanisms of solidarity to deal with what used to be called "providence". Rather than spreading the burden of risks, pre-emptive policies consist of looking ahead and acting as if the feared-for event had occurred and to immediately take in advance the necessary steps (refusal to insure a potential fraudster, preventive elimination of a potential terrorist, vocational-oriented guidance of children based on early profiling, etc.). Of course, depending on the areas in which it is applied, pre-emption may be appropriate to greater or lesser degrees.

Nonetheless, the fascination with Big Data and data mining as a means of assigning in advance to each person – in a very individualising way which involves no reference to any "average" calculated for a whole population – the "real" costs and opportunities relevant to him or her (in the field of security, health marketing, human resources, insurance, etc.), is perhaps not so much the consequence of a greater need for security than a change of response to the demand for security, which itself is in no way new.

In *The World of Yesterday*, Stefan Zweig, describes the golden age of security, the golden age of insurance in Vienna in the 1900s. In the security age, all forms of danger had not disappeared as if by magic, but thanks to statistics, people had learned how to domesticate, by means of calculating probabilities and pooling risks, what formerly would have been called providence and what today would be called uncertainty.

> "When I attempted to find a simple formula for the period in which I grew up, prior to the First World War I hope that I convey its fullness by calling it the Golden Age of Security… This feeling of security was the most eagerly sought-after possession of millions, the common ideal of life. Only the possession of this security made life seem worthwhile… gradually the great masses forced their way towards it. The century of security became the golden age of insurance… Servants saved up for old-age insurance and paid in advance into a burial fund for their own interment."

The "perfect" individualisation of risks and opportunities would, for example, mean the end of the raison d'être of insurance, the prime role of which is certainly not to individualise the burden of risks but rather to create limited "social contracts" between individuals, the insured, who, subject to comparable risks, undertook to bear collectively the cost of blows of fate dealt to certain of them. As François Ewald explains,

"Strictly speaking there is no individual risk, otherwise insurance would become a lottery or a wager. It is only when looking at the whole population that the risk becomes calculable. The work of the insurer is, precisely, to constitute that population by selecting and dividing."[42] He further explains that "insurance individualises, it defines each person as a risk, but the individuality it confers no longer correlates with an abstract, invariant norm (…) it is an individuality relative to that of other members of the insured population, an average sociological individuality." "Whereas an accident, as

playing this lack of understanding off against itself, negating it, as it were, by using it against itself. (Ewald F., *Histoire de l'Etat providence*, LGF - Livre de Poche; New revised edition (1 January 1996), p.114).

[42] *Ibid*, p.138-139.

damage, misfortune and suffering, is always individual, striking at one and not another, a risk of accident affects a population. Strictly speaking there is no such thing as an individual risk, otherwise insurance would be no more than a wager. Risk only becomes something calculable when it is spread over a population. The work of the insurer is, precisely, to constitute that population by selecting and dividing. Insurance can only cover groups; it works by socialising risks. It makes each person a part of the whole."[43]

In the light of these considerations relating to insurance, Big Data would, it seems, make it possible to move from an actuarial to a post-actuarial society in which solidarity among persons belonging to the same insured "population" is replaced by the possibility of individualisation and a fluctuation in real time of insurance premiums. The real-time and continuous adaptation of the premiums to be paid by each insured person depending on his or her day-to-day behaviour (driving quality, engaging in sport, dietary habits, etc.) could have socially desirable incentive (or dissuasive) effects but could also – by making it possible, for example, to evaluate the future state of health of individuals on the basis, for instance, of the record of their everyday consumer purchases (see below) – have harmful consequences for the principles of equal opportunities and solidarity. In this connection, the challenges of individualising premiums (or the hyper-segmentation of the insurance market in accordance with ever increasing individual and singular factors) posed by the Big Data phenomenon, are not fundamentally different from those raised by the provision to insurers, employers and other interested stakeholders of individual genetic data indicating a predisposition to certain illnesses among individuals currently in good health.[44]

Nonetheless, the "objectivity" of the algorithmic constitution of profiles, which no longer, on the face of it, targets any particular person, no longer presupposing any perceptual category, thereby being perfectly "egalitarian", can also make the modelling and classifications based on Big Data a phenomenon apparently independent of the systems of legal or traditional differentiations (depending on status, privileges, socio-economic advantages or disadvantages, etc.) identified by Boltanski and Thévenot as the foundation on which is based a model city, justifying or legitimising its "states of worthiness" and whose existence is both a precondition and an effect of relationships of power.[45] Similarly, while European law, in particular, recognises and protects a range of characteristics (gender, sexual orientation, disability, age, ethnic origin, national origin, religion or beliefs) particularly likely to expose those with those characteristics to discrimination, the discrimination which could potentially emerge in the Big Data world would be difficult to relate (at least directly) to those different characteristics. In other words, whereas for example, the European Directives in this field seek to prevent differences in treatment based on race or ethnic origin, religion or beliefs, disability, age, gender or sexual orientation, this category-based approach to discrimination would appear on the face of it to exclude differences of treatment based on data intelligence, and which, like the "a-signifying machines" described by Félix Guattari almost thirty years ago, "recognise neither subjects, nor persons, nor roles, and not even delimited objects. That is precisely what confers upon them a kind of omnipotence; they pass through signifying systems within which individuated subjects

[43] Ewald F., "Insurance and Risk" in Burchell G., Gordon C., Miller P. (eds.), *The Foucault Effect: Studies in Governmentality*, Chicago University Press, 1991, pp. 197-210.
[44] In this connection, reference is made to Rouvroy A., *Human Genes and Neoliberal Governance: A Foucauldian Critique*, Routledge-Cavendish, 2007.
[45] Boltanski L. and Thévenot L., *De la justification. Les économies de la grandeur*, Gallimard, 1991, p.162.

find themselves lost and alienated."[46]

In other words, the hyper-fragmentation and exponential growth of the digital world, offers new modelling possibilities – simultaneous rather than in advance of the processing of data – which are replacing the systems for perceiving and interpreting the world previously founded on representational phenomena (statistical representation, oral testimonies, symbolisation, institutionalisation, etc.) and for recognising preconfigured structures, forms, categories (politically, legally and culturally). For this reason, the radical reconfiguration of what Michel Foucault called "divisive practices"[47] by Big Data-type processing challenges – even more fundamentally than systems for the protection of privacy and personal data – the right to non-discrimination which has always been conceived in accordance with the existence of preconstituted human categories and groups that are clearly recognisable and, as such, particularly vulnerable to discriminatory practices.[48]

1.5. Conclusion of Part I

To talk of Big Data is to immediately evoke a change in approach in the detection, classification and predictive assessment of events in the world and of the behaviour and propensities of its inhabitants, i.e. therefore, a new way of making the world "predictable"[49] if it cannot be made "significant" (dispensing with the conventional processes of enunciation and validation) combined with new ways of exercising power: a new "governmentality".[50] Insofar as "data intelligence", reviving a sort of digital behaviourism, would gradually supplant the statistical, political and legal forms through which we represent what is real, we need to ask how the law will still be able to contain, limit and restrict the dominance of algorithmic governmentality, including over legislative and judicial processes.

To talk of Big Data is also immediately to evoke new prospects of technological innovation, new, increasingly personalised, services able to anticipate rather than simply react to the stimuli of the digital world. It is moreover striking to note that in the eyes of what is termed the "digital revolution", no doubt on account of the constant need for innovation having acquired the status of absolute imperative, individuals are most often described as "consumers" or "users" with promises of improving their experience, and much more rarely as "citizens".

Some stakeholders assert that in order to promote innovation and the fulfilment of the economic potential of Big Data, the application of certain fundamental principles of data

[46] Guattari F., *Révolution moléculaire*, Recherches, coll. Encres, 1977, p. 264.

[47] " (…) I have studied the objectification of the subject in what I shall call "divisive practices". The subject is either divided within himself or herself or divided by others. This process objectifies him or her. Examples are the division between the mad and the sane, the sick and the healthy, criminals and "good boys". (Foucault M., "Le sujet et le pouvoir", *Dits et Écrits II,* Gallimard, 2001, p. 1042.

[48] We shall see that Big Data approaches question the effectiveness of the current approach which consists, on the one hand, of prohibiting and preventing distinctions of treatment on the grounds of protected characteristics or vulnerable categories and, on the other, preventing any collective action by potential victims of discrimination based on algorithmic profiling.

[49] However, we need to find a different adjective from "predictable" insofar as, on the one hand, the relationship with the world brought about by Big Data dispenses with any relationship of the senses (in particular a visual relationship) with the world and, on the other, it is no longer so much a question of predicting in order to prevent than of detecting pure potentialities in the present and acting "in advance" as if they were already a reality. So it is no longer a question of "reacting" to the stimuli of the world but rather of anticipating events in the world by producing the appropriate stimuli.

[50] Regarding the concept of governmentality, see Foucalt M., "La gouvernementalité", in *Dits et écrits*, t.II, Paris, Gallimard, Quarto, 1994, 635–657; Burchell G., Gordon C., Miller P. (eds) *The Foucault Effect. Studies in Governmentality*, University of Chicago Press, 1991.

protection (in particular the principles of purpose limitation and data minimisation) should be relaxed in favour of a risk-based approach. The idea would be to significantly liberalise the collection of data and instead regulate the use of data, in an approach based on the anticipation of possible harm so as to promote responsible use of data. However, as the Article 29 Data Protection Working Party recently stated,[51] there was no convincing reason to believe that the fundamental data protection principles were no longer valid and applicable in the Big Data context, subject to further improvements to make them more effective in practice. The Article 29 Working Party also stated that complying with this data protection framework was a key element in creating and keeping the trust which any stakeholder needed in order to develop stable business models based on the processing of such data. In addition, compliance with these data protection rules and investment in privacy-friendly solutions was essential to ensure fair and effective competition between economic players on the relevant markets. In particular, upholding the purpose limitation principle was essential to ensure that companies which had built monopolies or dominant positions before the development of Big Data technologies held no undue advantage over newcomers to these markets.

First, the expectations generated by Big Data all converge on the prospect of improvement (in the sense of more objective and optimised) decisions in a multitude of sectors: security and prevention of terrorism; optimised distribution of the presence of police, healthcare, energy policies, traffic management and optimisation of public transport, fraud prevention, marketing and improvement of "consumer' and users' experience", price differentiation based on customer profiles, stock management, educational and training guidance, recruitment and human resources management, etc.)

Big Data opens up, for example, new expectations in terms of the "objective" planning of public policies. Collected via sensors installed in the roll-out of the concept of the "smart city" and via mobile telephony, Big Data offer the promise of taking an objective snapshot in real time of life in the city and its infrastructure, in the interests of development, management, regulations and life in the city based on data – i.e. in a digital, quantitative form of rational evidence. Big Data could, for example, help optimise the frequency, timing and routing of public transport depending on the collective interests deduced from geolocation.

However, the new capabilities of digital surveillance, pre-emptive analysis and automated decisions alongside the computational turn[52] also rekindle, crucially, the fundamental issue of the definition of the social contract between individuals, companies and states.[53] Presenting the issues in terms of innovation, competitiveness and the individual interests of consumers or users often hides the ethical, legal and political issues of the digital revolution at the risk of undermining the rule of law, human rights and fundamental freedoms, and preventing the striking of a fair balance between private and public interests on the one hand, and between those interests and the

[51] Statement of the Article 29 Working Party on the impact of the development of Big Data on the protection of individuals with regard to the processing of their personal data in the EU (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf)

[52] The metaphor of the "computational turn" evokes to an extent a transformation of the "linguistic turn": the unit of perception and understanding of the world is no longer the sentence, word or sign, always bearers of meaning, but a data item, a fragment which individually has no meaning but which is calculable, generated by rather than transcribing the world, "zero degree writing" if one may express it as such.

[53] We shall not here go into the issues relating to the shift towards crowdsourcing, which also questions the nature of the contract between individuals, companies and the state.

rights and freedoms at issue on the other. However, the new capacities based on "data intelligence", much of which remains imperceptible or inaccessible to the ordinary citizen, can significantly magnify the asymmetry of information and/or power between those who hold those data and those who, voluntarily or not, "emit" them.

In point of fact, one of the "added values" of the fundamental right to personal data protection compared with the fundamental right to protection of privacy is precisely that one of its objectives is to reduce the asymmetries in power and information between individuals and the natural or legal persons that collect, store and process data relating to them.[54]

Philip Agre provided a fairly convincing description of the objectives pursued by data protection instruments on the one hand, and the instruments for the protection of privacy on the other:

"Control over personal information is control over an aspect of the identity one projects to the world and the right to privacy is the freedom from unreasonable constraints on the construction of one's own identity".[55]

Accordingly, in order that an individual should have "control over an aspect of the identity one projects to the world", the protection of personal data provides individuals with a guarantee of the rights of control over data relating to them (a degree of informational self-determination) even if the processing of those data would not constitute a violation of the right to protection of privacy: the concept of personal data includes data relating to non-identified but identifiable persons, whether or not steps are taken to identify them (whereas the finding of a violation of the right to privacy presupposes at the very least that the person be identified).[56]

In view of the role of the protection of personal data in society,[57] particularly with a view to combating all forms of discrimination, and bearing in mind the need to reconcile data protection with other fundamental rights and freedoms, and also the need to take into account the indivisible nature of civil and political rights and economic, social and cultural rights, we shall now, in Part 2, look at how the Council of Europe's Convention 108 can help protect all natural persons in respect of the processing of Big Data.

[54] Lynskey O., "Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order". International and Comparative Law Quarterly, 63 (3), 2014, pp. 569-597.

[55] Agre Philip E., Rotenberg M. (eds.), *Technology and Privacy. The New Landscape*, MIT Press, 1998, p. 7. With regard to the distinction between the right to protection of privacy and the right to protection of personal data, see also Kokott J. and Sobotta C., "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", in *International Data Privacy Law,* 2013, 3 (4): 222-228. With regard to the overshadowing of the right to protection of privacy by the right to the protection of personal data in EU law, see González Fuster G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Springer, 2014.

[56] Friedl v Austria (1996) 21 EHRR 83

[57] The Court of Justice of the European Union, referring to its Schmidberger judgment of 12 June 2013 (C-112/00, Rec. p. I-5659, paragraph 80), quite rightly stated in its judgment of 9 November 2010, in the joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert (Rec. 2010, p. I-0000), that the fundamental right to the protection of personal data was not "an absolute right, but must be considered in relation to its function in society".

2 THE COUNCIL OF EUROPE'S CONVENTION 108 IN THE BIG DATA AGE.

2.1 Scope and definitions (Article 2.a.) - The concept of personal data

Personal data (meaning any information[58] relating to an identified or identifiable individual), which are the only kind whose automatic (or other) processing has been deemed to pose a sufficient threat to fundamental rights and freedoms to warrant legislation, do not always feature in Big Data-type processing.

There are some applications, such as those designed for climate analysis or monitoring oil rigs using data gathered by sensors fitted on the rigs, where no personal data processing occurs at any stage. Applications for predicting the outbreak and spread of epidemics (Google Flu), for discovering the side effects of drugs or for combating urban pollution do not involve processing personal data, provided the data have been carefully anonymised.

In other cases, personal data clearly do play a part in Big Data processing. Possible sources of such data include mobile phone applications, smart grids, in-vehicle transponders for calculating kilometre-based charges or for determining insurance premiums based on the distance covered, medical records, location data, social media, flight manifests, public records, loyalty programmes, DNA sequencing, purchase histories and also, increasingly, a plethora of "smart" objects (toothbrushes, fridges, footwear, watches, TVs, etc.) which not only enable their owners to be identified but also reveal much about their lifestyles.[59]

In such cases, data anonymisation is touted as a sufficient condition to relieve data controllers of their obligations and to deny individuals the privacy to which they are entitled by virtue of their right to personal data protection. However, as the Article 29 Working Party commented in its opinion of 10 April 2014, "[a]nonymisation constitutes a further processing of personal data; as such, it must satisfy the requirement of compatibility by having regard to the legal grounds and circumstances of the further processing. Additionally, anonymised data do fall out of the scope of data protection legislation, but data subjects may still be entitled to protection under other provisions (such as those protecting confidentiality of communications)".[60]

In essence, there are two issues that need to be addressed here in the context of Big Data. Firstly, the distinction between personal data and anonymous data is no longer clear now that the risk of individuals in anonymous databases being re-identified is considerable. And secondly, anonymity is no safeguard against the possibility of characterising individuals' behaviours or forecasting future behaviours.

- *The risk of individuals being re-identified through cross-referencing of anonymous data.*

A recent study by researchers at MIT showed that knowing just four random pieces of information was enough to re-identify 90% of people in an anonymous metadata set (containing

[58] To begin with, there is the issue of whether an item of data, taken in isolation, may be regarded as information or whether it is "merely" a signal, devoid of meaning yet quantifiable. Information could in that case be said to be the result of data processing.

[59] International Working Group on Data Protection in Telecommunications, Working Paper on Big Data and Privacy. Privacy principles under pressure in the age of Big Data analytics, 55th Meeting, 5 – 6 May 2014, Skopje.

[60] See Opinion 05/2014 of the Article 29 Working Party on Anonymisation Techniques, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

no names, addresses, credit card numbers or anything else than might be considered personal data) recording three months of credit-card transactions by 1.1 million users. Knowing the amount of just one transaction would increase the risk of re-identification by a further 20%. An earlier study had likewise demonstrated the feasibility of re-identifying people from anonymous location data.[61]

This ability to re-identify people from anonymous metadata arises from the wholly trivial fact that every individual has certain behaviour patterns of which they themselves may be unaware but which can be easily identified through their "digital footprint", provided the data are collected and stored over a certain period of time (three months in the case of the above-mentioned studies). In the age of Big Data, therefore, anonymity is entirely relative and hinges on the amount and variety of the data and the length of time for which they are stored far more than it does on the "information density" of each item.

a) Given the substantial risks of re-identification that exist with regard to anonymous data, is there perhaps a case to be made for treating anonymous data as personal data whenever they are used in Big Data-type processing that is liable to affect a person's socio-economic opportunities? There are a number of practical obstacles to such an approach. For example, how do we determine at what point an anonymous piece of data starts to play a part in constructing a "profile"? Also, how to identify in advance (i.e. before the purpose of the profiling exercise has been achieved) the individual who "owns" the data?

b) Another more feasible approach would be to require any entities wishing to anonymise data to carry out a prior assessment of the re-identification risks (based on the amount and variety of the data and the length of time for which it is proposed to store them) and to communicate the results to the individuals concerned before seeking their consent and indeed at any time if there was an increased risk of re-identification. Such an approach can be seen in the wider context of the requirement for a privacy impact assessment and the requirement to adopt technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing referred to in Article 8bis§2 and§3 (additional obligations) of the (modernised) Convention 108. This is, of course, far from a perfect solution. One of its drawbacks is tied up with the temporal aspect of the issue of re-identification. Data that are anonymous today may lose their anonymity in the future because it may be possible to cross-reference them with other data collected either by the controller of these autonomous data or by a third party. The risk of re-identification shifts considerably over time. Any risk assessment cannot therefore be carried out once and for all; risks need to be regularly reviewed or permanently monitored, and this is made all the more difficult by the fact that it is hardly conceivable to draw up a list of all current and future data liable to be cross-referenced with anonymous data in the controller's possession. Nonetheless, although inadequate, requiring a risk assessment when data are anonymised and possibly combining this with a requirement for a regular review has the advantage of alerting both data subjects and data controllers to the fact that anonymity is never fully guaranteed and encouraging them to exercise caution when giving consent in the case of the former or, in the case of the latter, allowing anonymous data in their possession to be cross-referenced with other sets of data in their possession or the possession of third parties.

In all cases, the mere argument that the processed data were anonymous data is not sufficient to absolve data controllers of all responsibility but, on the contrary, given the risks of

[61] de Montjoye Y.-A., "Unique in the shopping mall: On the re-identifiability of credit card metadata", *Science* 347, 30 January 2015; de Montjoye Y.-A., Hidalgo C. A., Verleysen M. and Blondel V. D., "Unique in the Crowd: The privacy bounds of human mobility", *Nature Srep.* 3, 25 March 2013.

re-identification, they should be obliged to take all the necessary technical measures to minimise those risks.[62]

- *Anonymity is no safeguard against the possibility of characterising individuals' behaviours or forecasting future behaviours.*

Since "models" or "profiles" are built from data derived from large numbers of people, and since one person's data are no less (in)significant than another's when it comes to modelling, only a small amount of not-very-personal data are needed to produce "new" knowledge about any given individual, i.e. to infer certain pieces of information that bear no immediate relation to "their" personal data but which nevertheless enable them to be "categorised".[63] In other words, when it comes to building a "profile", in order to be able to "capitalise" on the risks and opportunities that we present, our neighbours' data are as good as our own. Should it be considered then that everyone has a right of ownership over data relating to their neighbours insofar as harvesting and processing those data carries a risk that they themselves will be able to be identified or assigned a particular profile? Among other things, this would mean the same information could be claimed by multiple individuals as "their" personal data, which would be completely unmanageable, of course.

This need to bring the discussion back to issues of personal data protection is indicative of an individualistic methodology that might not be the most appropriate for the issue that concerns us here. The types of power at play in the age of Big Data are perhaps exercised far less through personal data processing and identifying individuals than through algorithmic forms of constantly evolving, impersonal categorisations of risks and opportunities, in other words of the way people live (attitudes, movements, etc.). A profile is not, in reality, about any one person. No-one fits it exactly and no profile pertains to a single identified or identifiable individual. Being profiled in this or that way, however, affects the opportunities that are available to us and consequently the realm of possibilities that defines us: not only what we have already done or are doing, but also what we could have done or could do in the future.[64] As demonstrated above, moreover, with the advent of Big Data, the value of any given piece of data is essentially relational in nature, rather than intrinsic: it is the (cor)relations between data that makes them valuable and useful, and perhaps also sensitive, to a greater or lesser degree.

The challenge facing us now may therefore be framed as follows: how to take account, in personal data protection instruments, of the relational, and therefore also collective, nature of what, through data, merits protection?

2.2 Basic principles: legality and good faith, purpose and proportionality, accuracy.

- *Consent **(Article 5§2)***

Under **Article 5§2** of the (modernised) Council of Europe Convention 108, data processing may be carried out only on the basis of the free, specific, informed and unambiguous **consent** of the data subject or some other legitimate basis laid down by law.

[62] See also Narayanan A., Huey J. and Felten E. W., "A Precautionary Approach to Big Data Privacy", March 19, 2015, CPDP proceedings, http://randomwalker.info/publications/precautionary.pdf
[63] van Otterlo M., "Counting Sheep: Automated Profiling, Predictions and Control", paper presented at the Amsterdam Privacy Conference from 7 to 10 October 2012.
[64] In this respect, see Hacking I., "Making Up People", *London Review of Books*, 2006, vol.26, no.16, pp. 23-26.

In the case of the personal data involved in Big Data-type processing, the protective nature of the requirement for free, specific and informed consent is liable to be less effective[65] when the consent to the collection and processing of these data is presented in what are often standard form contracts as a precondition for using certain devices, services or applications, or when certain connected devices are offered free of charge provided their users agree to the personal data captured by these devices being collected and processed. The issue then becomes one not so much of informed consent as of whether it is acceptable to relinquish the right to personal data protection, a right that is recognised as being fundamental.

It seems, furthermore, that most of the time, when individuals consent to the systematic collection of these "soft data", they do so almost automatically. There are a number of reasons for this: the "nothing to hide and therefore nothing to fear from surveillance" argument coupled with the convenience of immediacy and the perceived benefits of interaction and personal exposure far outweigh concerns about loss of privacy or disclosing personal data. This is especially true given that erasing one's digital footprint requires individuals to make an active choice (opt-out), when, as is often the case, "choice architecture" involves (opt-out) default registration rules.

In this respect, the *success* of data storage default rules or, to put it another way, the lack of success of the various options for overriding such rules, can be attributed, as Cass. R. Sunstein[66] argues, drawing on behavioural economics, to a combination of three principal factors: The first factor is the inertia that occurs when erasing our "digital footprint" demands an effort whose rewards are not really certain or clear, given that each piece of data generated by our online activities seems at first sight (irrespective of any cross-referencing or modelling operations to which they might contribute) to be of little importance. The default rule, even when we have the ability to override it very easily "in just a few clicks", will always prevail if the particular issue at stake, there and then, does not appear significant in the eyes of the internet user. The second factor in the success of default rules where data storage is concerned is that when they are unsure which is the right course of action, the average user will tend to assume that, because it was devised by somebody else with greater expertise than themselves, and because the majority of other people probably accept it, the default rule is no doubt the best option for them too. The third and last factor has to do with the fact that people are typically more sensitive to the *risk of losing* an advantage which they already enjoy, or believe they enjoy, under the status quo than to the *opportunity of gaining* something by changing. This is a variation of the inertia phenomenon but one through which designers and marketing professionals can acquire control over individuals: they can reduce the probability of users opting out of the default rule to protect their privacy by reminding them of everything they stand to lose, as retaining users' "digital footprints" is what enables businesses to provide those same users with a more personalised service, one more appropriate to their real-time needs based on where they are, or their particular tastes, a service that is faster and better. Reminding users that erasing their footprint will cause them to lose all these advantages is usually enough to deter them from opting out.

[65] For a criticism of the principle of consent in the context of predictive behaviour modelling based on Big-Data type analyses, see Mantelero A., *The future of consumer data protection in the EU. Rethinking the "notice and consent" paradigm in the new era of predictive analytics*. Computer Law and Security Review 2014, (30):643-660.

[66] Sunstein C. R., "Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules: A Triptych", 19 May 2013, http://ssrn.com/abstract=2171343

A recent study[67] suggests, however, that, contrary to what the marketing industry would have us believe, in consenting to the collection and storage of data culled from their online activities, internet users are acting not so much out of a belief that there is something in it for them, by agreeing to trade data derived from their online activities for various benefits (e.g. discounts), as out of a sense of resignation about what they see as an inevitable loss of control over their personal information – a feeling that is reinforced if not actually brought about by announcements of "the end of privacy", emanating mainly from certain key players on the web who benefit from this resignation and propagated abundantly by the media.

The fact remains that because, amongst other things, of the default settings of digital devices and applications software (which keep, for example, users' internet browsing history unless the user expressly indicates otherwise), it is more by default than because they have given their free and informed consent that individuals are contributing to this proliferation of data stored "in the clouds", i.e. a long way from the device itself yet, contrary to what this nebulous metaphor suggests, not in a dispersed fashion but in a highly centralised one, in vast data centres.

Because individual autonomy, if there is such a thing, is not a purely psychological capacity but rather contingent on socio-economic, educational and design factors, individual choice "architecture", such as systems of default rules, based on the lessons of social psychology or on algorithmic detection of the psychological profile of what is termed "the user", should be subjected to rigorous scrutiny, especially when such architecture is devised by actors whose interests do not match those of the "users". The urgent importance of developing a typology of the various players involved in digital media and, above all, of their "interests" cannot be overstated. This seems to me a more promising route at present than stubbornly insisting on a purely illusory requirement for free and informed consent.

Choice architecture built by players whose interests do not coincide with those of the user, encouraging, in the ways described above, the user to refrain from opting out, are apt, in practice, to be incompatible with what Henri Atlan, for example, calls "the minimal experience of choice" which

"implies that a number of alternatives are offered and *that choice is the deciding factor* whereby one of those alternatives is realised, thereby moving from the status of 'possible' to the status of 'real', or, more accurately 'current'". [68]

It is clear from the above (the ease with which trade-offs can be made, i.e. consenting to data processing in exchange for various benefits, and the "power of choice architecture" over individual decisions) that the requirement for consent provides very little protection for individual and collective interests under potential threat from Big Data. Consequently, a much clearer picture of the prerequisites for "free, specific, informed and unambiguous consent" would have to be provided, stating in particular that controllers must guarantee that personal choice is the deciding factor (to the exclusion of any offers of benefits in exchange for consent, and to the exclusion of any tinkering with choice architecture in order to obtain consent) by which individuals consent, or do not consent, to the processing of their data. It might also be advisable here to encourage controllers to adopt *opt-in* rather than *opt-out* systems so as to reinforce the unambiguous nature of consent.

[67] Turow J., Hennessy M., Draper N. "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation", A Report from the Annenberg School for Communication, University of Pennsylvania, June 2015.

[68] Atlan H., *Les étincelles de hasard,* T. 2., Seuil, 2003, *p*. 77.

In addition to the requirement for free, specific, informed and unambiguous consent, Big Data-type processing seems to run directly counter to the principles of data minimisation and purpose limitation.

- *Data minimisation (**Article 5.4.c)***

Since, as explained above, the actual usefulness of any piece of data, including personal data, depends on the amount of other data collected with which it could be aggregated, controllers will necessarily tend to keep them not only whenever they are helpful or essential for the provision of a particular service but also over and above what is strictly necessary for the services they offer their clients. Accordingly, even though there can be no justification for mobile phone operators geographically tracking users outside those periods when the user has specifically activated a particular application (automatic recommendation systems for nearby restaurants, for example) that necessitates tracking, it is actually very difficult for users to ensure that their data are processed in line with the operator's specific obligations and in accordance with the law because, of course, all this takes place in a way that is neither visible nor apparent to the user.

It would be a good idea here to improve the effectiveness of the requirement to report data processing operations (to the data protection authorities) and also, as already mentioned above, the requirement to inform data subjects, including in cases where the purpose of the processing is not defined as anything other than to develop data sets large enough to provide the basis for Big Data-type processing.

It might also be advisable to make the establishment of anonymised databanks for the purpose of carrying out Big Data-type processing subject to approval by the data protection authorities.

- *Purpose **(Article 5.4.b)***[69]

Similarly, it is doubtful whether users of certain social networks, in formally consenting to their data being stored for the purpose of research and network functionality improvements, genuinely intended to allow themselves to be used as "guinea pigs" in social psychology experiments conducted across that same network and which involved manipulating their emotions by filtering, over a certain period of time, users' news feeds in order to see how relatively prolonged exposure to pessimistic, negative, alarmist content, etc. affected their mood. This time it was the principle of purpose that was undermined but the latter is also, of course, inimical to the whole philosophy of Big Data, driven as it is by the constant need for innovation, now elevated to the status of absolute imperative, and which dictates that no curbs be placed on the ability of Big Data to produce new goods and services thanks precisely to the availability of massive amounts of data whose growth must not be inhibited by any concerns about purpose.

1. It seems there is a need to explore the distinction, which appears to be rather blurred in people's minds, between freedom of scientific research and the need for innovation. While this is not the place for that discussion, which would lead us too far from the subject of data protection, we would nevertheless point out that freedom of scientific research is one of the values taken into account in Convention 108 when it provides, in Article 9 (exceptions and restrictions) for the possibility of restricting data subjects' rights with regard to data

[69] On the principle of purpose, see *Opinion 03/2013 on purpose limitation* of the Article 29 Data Protection Working Party, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

processing operations which pose no risk. The example given is that of the use of data for statistical work, insofar as these data are presented in aggregate form and stripped of their identifiers. Similarly, scientific research is included in this category. It stands to reason that a distinction needs to be made between Big Data-type processing and data processing for statistical purposes. It has been explained above how Big Data processing operations involve new statistical methods which are different from conventional ones. Furthermore, the condition for statistical processing operations to be exempt is that they must "pose no risk" for the individuals (as explicitly stated in the Explanatory Report on Convention 108). With Big Data-type processing, however, the possibilities for personal profiling, including predictive profiling, coupled with the potential for automated decision-making with regard to individuals (see Part 3 below) certainly do carry a risk for the persons concerned. The "freedom to innovate", on the other hand, is not one of the values implicitly or explicitly protected under Convention 108, nor is it among the fundamental rights and freedoms enshrined in the European Convention on Human Rights.

2. The principle of the purpose of personal data processing needs to be very firmly reiterated, therefore, and, where appropriate, extended to anonymised data, in line with the above comments on this subject.

- *Principle of fairness and transparency of data processing (**Article 5.4.a)***

[There may be some repetition between the requirements for transparency provided for in Articles 5.4.a and 7bis of the revised version of Convention 108 on the one hand and Article 5.2 (on the requirement for free, specific, informed and unambiguous consent, which necessarily also entails a requirement of transparency) on the other. Given this, we would suggest that Article 5.4.a. should be reworded as follows: "a. processed fairly with regard to the data subject".]

It should perhaps be emphasised here that the requirement for fairness applies to all data processing including collection (see above) and any anonymisation carried out (in which case fairness would imply in particular that an assessment of the risks of re-identification should be carried out and the data subject informed of the results of the assessment).

- *Principle of limits on the length of preservation (**Article 5.4.e)***

Because of the risks of re-identification through cross-referencing of anonymous data, anonymisation is not enough on its own to absolve data controllers from all obligations towards data subjects. Furthermore, controllers should be required among other things to ensure that the anonymisation techniques they use are in keeping with the latest developments in the field. Insofar as the risk of re-identification may increase over time and as a result of progress in re-identification techniques,[70] the principle of time limitation – including, where appropriate for anonymised data when anonymisation techniques can offer no guarantee against the risk of re-identification – needs to be reasserted, perhaps even more in the Big Data context than in others.

2.3 Sensitive data (Article 6)

Among the various kinds of data used in Big Data-type processing, data that are sensitive (e.g. data which reveal information about a person's racial origin, political opinions, religious or

[70] See Opinion 05/2014 of the Article 29 Working Party on Anonymisation techniques, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

other beliefs, data about health or sexual life, genetic and biometric data, data relating to trade union membership, criminal convictions, offences and other penal measures) either inherently or *because of how they are used*,[71] are not a minority category. Pictures of individuals provide information about their ethnic origin and profiling people based on the kinds of films and entertainment they like (Netflix, on-demand TV, etc.) provides clues to their political opinions and/or their religious beliefs, just as tracking supermarket shopping habits can also provide information about customers' current and future health status, or their religious practices.

Deloitte accordingly explains that it is possible, using a supermarket shopping database, to determine a person's current and future health status with a degree of accuracy comparable to that of a medical examination. These "consumer profiles" are apparently sufficient to detect individuals' propensity to develop diseases such as diabetes, women's cancers, smoking-related cancers, cardiovascular disease, depression, etc.[72] Whereas traditionally, people wishing to take out insurance have had to declare only pre-existing conditions, diseases and disabilities of which they are aware, the fact that insurers might in future be able to detect diseases and propensities for diseases in their customers, without the latter even knowing about their condition, would create an information asymmetry highly detrimental to the insured persons.

In the hyper-connected world we live in, according to calculations performed by IBM, each person generates more than one million gigabytes of health-related data over their lifetime. These health-related data are no longer produced only by doctors, hospitals or health insurers, but also by the individuals themselves, whether they are ill or not, thanks to the growing popularity of connected gadgets for monitoring physiological parameters such as heart rate, or the number of calories burned each day, etc. Data about diet, gym attendance, or how often people visit health-related websites or discussion forums, etc. can all potentially be classed as data relating to current or future health. If we also include the data produced through human DNA sequencing, which amounts to tens of terabytes per genome, it is clear that health-related data play a major part in Big Data. As, thanks to Big Data, correlation upon correlation[73] emerges between what, at first, might seem to be non-health-related information and the onset of various diseases or disabilities (lifestyle, eating habits, climatic and environment factors, etc.), the list of data with the potential to become sensitive through use grows to include types of data which before would never have been considered sensitive. If health-related data demand particular attention, it is because, of all the different types of Big Data, this is the fastest-growing segment, thanks, among other things, to flourishing new markets in "connected health".

Conversely, one effect of Big Data-type methods in the field of security and fraud prevention is that the value and usefulness of "visual" data such as those which may disclose a person's ethnic origin for example are greatly diminished. The algorithmic visualisation of the subtle connections between data makes possible unexpected discoveries and, in this respect, would liberate us from the constraints of human perception, ever biased and incomplete, always too context-bound, clouded by prejudice and resistant to novelty, in favour of an "automatic

[71] According to the distinction introduced in Article 6 of Convention 108 by the Ad Hoc Committee on Data Protection (3rd meeting, 1-3 December 2014).

[72] Rieke A., Robinson D. and Yu H., *Civil Rights, Big Data and our Algorithmic Future*, A September 2014 report on social justice and technology, Upturn

[73] "Correlation is what quantifies the statistical relationship between two values (correlation is said to be strong if there is a good chance that a value will change when another is altered and is said to be weak when a value has little chance of changing when another is altered", Karesenty J.-P., "Big Data (mégadonnées). Une introduction", *Revue du Mauss permanente*, 1 April 2015).

curiosity" free from preconceptions and capable of constantly adjusting its modelling as new data keep flowing in.

It is important here, in order to appreciate fully what is at stake, to make a clear distinction between two separate ways of categorising individuals and/or their behaviour. In the traditional processes of classification which it was possible to conduct before the digital revolution and the new Big Data-type assessment techniques, the categories (statistical, social, cultural and others) existed before the categorisation procedures, which consisted in looking at these pre-existing categories and working out which features could be used to identify or predict that a person belonged to a group and hence to place that person into the corresponding category. In the categorisation process, the actual circumstances observed were subsumed into pre-existing categories following a deductive line of reasoning. Individuals identified or recognised themselves consciously (as being part of a group of pupils' parents, for example, or a group of members of a particular association or people regarding themselves as belonging to an ethnic group, a political movement, a religious community or a gay/lesbian/queer movement) or were identified by others (as with censuses or incorporation into statistical categories) as belonging to a group because of certain common traits shared by the whole group. In the European Union, anti-discrimination directives prohibit discrimination when it is based on a person's membership of one or more categories which it lists: nationality, sex, ethnic origin, religious belief, disability, age and sexual orientation. These "protected characteristics" are the result of a realisation that the membership criteria which define them are more liable than others to expose those to whom they apply to unfavourable differences in treatment.

The aim of the processes of group profiling or clustering on the other hand is to highlight previously unknown, socially and visually imperceptible categories on the basis of data analysis without any reference to pre-existing information about these new groups or categories. In clustering processes, individuals are placed by another person – which can be an automatic data processing system – into socially and existentially a-significant "categories", which are imperceptible (because they emerge only as the process unfolds), and most often without any possibility of being aware of what is happening or recognising themselves. If we had to characterise these human "groupings", we could therefore make an initial distinction between categories in which individuals categorise themselves or can at least recognise themselves, in other words groups which to a greater or lesser extent are self-organising – in which there can be ties of solidarity, loyalty and interdependence along with the possibility of defending the group's interests – and groups in which individuals are categorised by others and are generally unaware that they belong to the "category" in question. This is the entire thrust of the distinction to be made between categorisation and clustering.[74] Categorisation unquestioningly subsumes perceived reality into pre-established categories, which are the result of political, cultural, aesthetic and ideological processes, in other words a specific perception and interpretation of the world whereas clustering is the automatic, "almost natural" result of the statistical processing of "data", which take on the appearance of "facts". Anti-discrimination systems cannot easily be applied to differences in treatment based on this type of grouping process as it can be claimed that by definition it is not because people belong to one protected category or another that they are treated differently but because of imperceptible modelling processes.

The presumed advantage of clustering processes over categorisation processes is therefore precisely the fact that they are socially, politically and ideologically "neutral" and that they bypass the inevitably "biased" categories through which we human beings are predisposed to perceive the world. This, incidentally, is one of the arguments frequently advanced for replacing

[74] Custers B. H. M., *The Power of Knowledge. Ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Tilburg: Wolf Legal Publishers, 2004.

airport security staff and customs officers with automatic devices that use profiling informed by Big Data. The "blindness" of Big Data-type processing to socially determined and discriminatory categories, and hence their impartiality, is, argues Tal Zarsky, one of the more problematic reasons why the majority, with its "appetite" for discrimination, is so averse to data mining: the individuals who make up "the majority" prefer that the burden (in terms of costs and disadvantages) of surveillance be shifted to smaller, specific groups which have no political power, rather than that they too should have to suffer a system of surveillance that would subject everyone to scrutiny in equal measure (under a "veil of ignorance" as it were). The expectation, then, is that Big Data-type approaches would lead to greater equality and prevent discrimination.[75] As we will see below, however, such methods are not proof against indirect discrimination and indeed can even exacerbate the problem insofar as "the data" are themselves a fairly accurate reflection of the social norms which operate in the physical world but which are rendered "undetectable" by the sheer volume of data (the issue of indirect discrimination will be addressed later).

The question then is as follows: is an approach that involves simply enumerating sensitive categories (and hence data) the most appropriate one for preventing discrimination in an era when, firstly, even the most trivial aspects of everyday life are potential indicators of a person's current or future health status and other sensitive characteristics and, secondly, differences in the way people are treated can take increasingly subtle forms, and be based not only on their membership of a particular historically discriminated-against group but also on particular features of their lifestyle?

2.4 Data security (Article 7)

Because the risks of personal data "leaks" as a result of security shortfalls in the systems of data collection, storage and processing are liable among other things to undermine individuals' confidence in the "digital economy" and therefore to reduce business opportunities and income accordingly, this field is one where there is major investment by the operators and regulators of the digital economy. For all that, making data processing secure is a particularly difficult task in the light of developments such as the fragmentation of data ownership and their distribution in time and space, the great variety of connected devices, the diversity of the stakeholders and the spread of cloud computing applications.

In the context of Big Data, the risks of re-identification of the persons concerned on the basis of anonymous or anonymised data would warrant making it an obligation for the data controller and, where appropriate, his or her subcontractor to take appropriate security measures (including technical measures in the areas of cryptography, access control and registration and automatic saving functions) to counter risks such as accidental or unauthorised data access – including anonymous and anonymised data – and destruction, loss, amendment or disclosure of data.

The supervisory authorities (provided for in **Article 12bis**) should be encouraged to co-operate with one another (through the exchange of information provided for in **Article 12bis7.a**) to prepare, update and disseminate to the public recommendations on the most recent data processing security methods.[76] Accordingly, the following sub-paragraph could be added to

[75] Zarsky T., "Governmental Data Mining and its Alternatives", 2011, *Penn State Law Review*, Vol. 116, No. 2: "if data mining is accepted by the legislature, it might only require limited judicial review. This is as opposed to the use of profiles and field officer discretion, which calls for greater scrutiny."

[76] See for example the recommendations issued by the Belgian Committee for the Protection of Privacy: http://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2013_0.pdf

Article 12bis 2.e. "(iv) measures to provide recommendations to controllers on state-of-the-art data processing security methods. For this purpose, the supervisory authorities are encouraged to exchange all relevant and useful information between one another."

However, as has been shown, the challenges of data security are not isolated to Big Data-type processing. In the Big Data universe, the main threat to fundamental rights and freedoms including economic and social rights stems not so much from ill-intentioned actions or culpable negligence (giving rise in particular to security failures) as from a new way of thinking by governments in which they base most of their decisions exclusively on "data intelligence". The widespread use of algorithm-based processing, which is used in good faith by public services and private companies, or the combination of well-intentioned bureaucracy and algorithms poses much more specific challenges which are quite different from those connected with security breaches.

2.5 Transparency of processing (Article 7bis)

Under **Article 7bis** of the revised version of Convention 108, controllers are required, in accordance with the principle of transparency of data processing, to inform data subjects of:

- their identity and their habitual residence or establishment;
- the legal basis and the purposes of the intended processing;
- the categories of personal data processed;
- if any, the recipients or categories of recipients of the personal data; and
- the means of exercising the rights set out in Article 8 [see below], as well as any necessary additional information in order to ensure fair and transparent processing of the personal data.

It would seem only right, in the age of Big Data, that the duty to inform data subjects should include information about the intention to re-use the data, even if only in anonymised form, for purposes other than those explicitly stated at the time of obtaining consent. As mentioned above, moreover, this duty to inform could arguably be extended to include the (quantifiable) risks of re-identification in situations involving the processing of anonymised data. After all, only if data subjects are aware of these risks will they be in a position to give their informed consent.

Lastly, to avoid unfair competition and excessive imbalances in the information available, it seems reasonable that, whenever it is planned to carry out Big Data-type processing in order to adapt marketing strategies or to customise commercial offers (by varying the price or quality of products, or by offering bonuses) according to behavioural traits, lifestyle or any other individual characteristic detected via Big Data analysis or by tracking people's activities and movements, the individuals concerned should be alerted to this by means of a clearly visible/perceptible margin note in the marketing material and, at the very latest, when the personalised offer is made.[77] Presenting these processes in terms of "improvements to services or customer experience" is frequently inadequate and misleads customers about the true purpose of the operation, which is to adapt the offer or the commercial conditions to the customer's "profile" (as the true aim of the operation is not to provide customers with something more useful or to increase their well-being but to maximise the company's profits).

[77] Executive Office of the President of the United States, *Big data and Differential Pricing*, February 2015, https://www.whitehouse.gov/sites/default/files/docs/Big_Data_Report_Nonembargo_v2.pdf

2.6 Rights of the data subject: decisions based on automated processing of data (Article 8)

A**rticle 8** provides in particular that:

> Every individual shall have a right:
>
> not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having their views taken into consideration;
>
> …
>
> to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her.

- *The prescriptive force of automated systems.*

The "prescriptive force" of the result of data processing (in other words the degree to which modelling and the "behavioural predictions" it produces are mandatory, persuasive or incentivising in nature) depends on several factors.

First, *factors tied up with the purpose of the system*. Is it a system designed to help with the decision-making process, a recommendation system or a system taking the place of human decision-making? The binding force of results of data processing depends, of course, on the purpose of the system (informational support, recommendation or decision).

Factors tied up with the "material" functioning of the system. Is it only technically possible to disregard the recommendation without delaying or preventing any action? For instance, one could imagine an "intelligent" car which would "refuse" to start until all the passengers have fastened their seatbelts. This type of system is intrinsically prescriptive: disobeying the order (to fasten one's seatbelt) would mean not being able to use the object (the car). Another example would be the automatic detection of suspicious behaviour in airports which, instead of "merely" alerting the security staff, would immediately shut down all lifts and escalators and close all the doors to areas that are open to the public. If the staff concerned were to ignore the alert in such a case, this would be tantamount to closing down the airport completely. When the procedure is triggered off, they are therefore compelled, almost physically, to take action, regardless of what their own assessment of the situation might have been.

However, even in the case of systems which are simply designed to make recommendations and do not replace human decision-making, *factors relating to the organisation of work and the evaluation of productivity or, in short, the management context* in which the decision-making process takes place, together with *factors relating to the psychology of human operators* required to heed or disregard the automatic recommendation (such as their degree of aversion to risk, the extent to which they will take individual responsibility for their actions, their inclination to obey or to resist orders to speed up the decision-making process) may considerably increase the prescriptive force of the automatic recommendation, which may, in some (rare) cases be ignored or by contrast (and probably in most cases) almost automatically and completely transposed into the human operator's decision. Therefore, it is conceivable that in quite a number of cases, the human operator will find it difficult to disregard the automatic recommendation, because on the one hand this is likely to reduce his or her level of productivity and on the other, it will oblige him or her to take personal responsibility for the decision and its consequences and to justify it in the event of a negative outcome, whereas a decision in keeping with the recommendation would have enabled him or her to shift the blame on to the computer system. Consequently, the very existence of an automatic recommendation gives rise to a duty, for those who decide to disregard it, to justify their non-compliance not "on their

honour and conscience" or based on any concept they may have of fairness or justice, taking account of the actual circumstances in which their decision had to be taken, but on the basis of arguments which are at least as quantifiable as algorithmic predictions. The clear implication of this is the elimination of the very concept that some things simply cannot be decided or are fundamentally uncertain – the concept which obliges judges to come down on one side or another, even though they know that justice can never be anything other than a governing ideal, which cannot be achieved by calculation alone. What is also done away with is any opportunity for human operators to disregard the "optimum" decision because of some incalculable and unforeseeable impulse towards clemency, generosity or solidarity, none of which can be justified by quantitative arguments alone. Lastly, what may ultimately fade away, for want of being used, is human operators' individual ability to assess the cases and situations they encounter themselves. This new form of "proletarisation"[78] – or loss of skills – brought about by automated decision-making systems makes human operators deeply dependent on their tools, at the risk – in the event of a technical breakdown – that they will be incapable of taking any decision.

- *Automated decisions and the ability to challenge decisions. What should be challenged: the facts or the circumstances surrounding the facts?*

If we regard all of this as an established fact and if we also wish to see it not so much as a danger but as a step forward (speeding up decision-making processes and making them more objective, avoiding the bias, prejudice and errors of judgement which are always possible when humans deal with situations, reducing security staff costs in highly frequented public places, etc.), it will be tempting to see the potential threats to fundamental rights and freedoms only in terms of possible machine errors caused either by the fact that the data being processed are false or incomplete (although the basic theory of Big Data – based partly on an ideological viewpoint – is that they have an aura of exhaustivity, see p. 11) or by the inadequacy of the modelling system (such as assumption-based errors, see p. 13). Yet the concept of machine errors presupposes that there is an "objective truth" equating to the facts themselves, which would *necessarily* have been found had it not been for the error or errors (which are also assumed to be detectable and rectifiable, which, as we have seen (p. 13) is far from obvious). The argument assumes that there will always be a perfect match between the facts, as perceived through their digital transcription, and justice, which is simply the transposition of the facts into a decision. This, of course, overlooks the fact, as Georges Canguilhem wrote, that "facts do not have any value in themselves. Indeed, as soon as they exist as facts they carry with them their own circumstances. Whoever knows the circumstances will change them. Therefore facts reflect not what one does but what one does not do."[79] No longer seeking to understand the causes of phenomena and attempting instead to make predictions on a purely statistical, inductive basis, in other words one which totally ignores causes, equates to no longer seeking to understand and change *the circumstances surrounding facts*.

As long as rational algorithmic thinking makes it unnecessary to question the reasons why, for example, in databases obtained from a region's employers, we find more women or people designated as belonging to a particular ethnic group among employees forced to leave the workforce early or not promoted, the cause (discriminatory trends in society) will be completely hidden when this procedure is used to develop employability profiles, which are granted the status of "objective facts". The practical deduction or automated recommendation to human resources managers will be as follows: "persons belonging to certain ethnic groups and women are statistically less successful professionally", but the discrimination, which is not always

[78] See, in particular, Stiegler B., *La société automatique*, *1. L'avenir du travail*, Fayard, 2015, p. 43.
[79] Canguilhem G., "La mobilisation des intellectuels: protestations d'étudiants", *Libres propos*, 20 April 1927, p.54.

necessarily formally identified as such because not everyone takes legal action for unlawful discrimination, but which is the *circumstance* underlying this *"fact"*, will no longer be perceived as a problematic issue.

This is the perfect illustration of something we have alluded to previously, which is that Big Data-type analyses lay claim to a form of objectivity[80] – not a *critical* form of objectivity based on the knowledge of the circumstances, the context and the causes of phenomena and hence on an acknowledgment of their contingent nature, but a *mechanical* objectivity, based on the one hand on the automation of data processing systems and a disregard of subjectivity (selectiveness, specific viewpoints,[81] perception, interpretation) and, on the other, the apparent independence of algorithmic modelling vis-à-vis politically instituted or socially experienced categorisations.

Yet, even when, or perhaps particularly when, they are self-learning, algorithms incorporate certain "world views", including those that tolerate discrimination, and also enable differences in treatment in the employment field to be carried out in accordance with highly opaque factors and criteria (even in the eyes of those who use algorithms for selection purposes) or within themselves, individually, for reasons unconnected with the requirements of the post or the job. Yet the impenetrability of algorithmic processes and the fact that they are covered by industrial secrecy make any discrimination very difficult to prove, especially as, most of the time, the intention to discriminate does not lie at all with the people who simply use these automatic systems to make their own decisions more objective. Indirect discrimination resulting from the operation of an automated recommendation system stems not so much from the person who decides to follow the recommendation (in fact, it might be said that this person's willingness to make his or her decisions more objective reflects a desire to cancel out his or her own prejudices) as from the prior existence in society of a discriminatory mindset (an "appetite" for or acceptance of discrimination) varying in scope but reflected passively in data sets and hence acquiring the status of an objective, apolitical, neutral and unproblematic fact.

One possible solution therefore may be to require considerably more than the mere possibility for persons significantly affected by a decision taken on the basis of automated data processing to assert their own viewpoint. Everything would tend to indicate that such viewpoints would have little weight when compared to the anticipated objective algorithmic findings of automatic systems. Furthermore, at an earlier stage in the process, the influence that individuals can have on profiling is very limited. The predictive models or supra-individual profiles assigned to individuals are based on infra-individual data deriving from a large number of individuals. In this process, data from any individual is just as valid as data from any other – *your data is as good as your neighbours* – meaning that only very little data is needed to infer new knowledge. Any relevant statistical information concerning individuals will already have been included in the model well before they can submit any information about themselves. The model literally forgets that individual "people" are concerned.

In addition to requiring it to be possible for data subjects to assert their own point of view, the main goal should be to require that due reasons be given for any decision based on automated

[80] A form of objectivity which derives from the relative non-selectiveness of its relationship with digital data, the independence of algorithmic modelling vis-à-vis socially established and experienced categorisations and the minimisation of human intervention in favour of automatic processes.

[81] However, algorithmic modelling take account of only what has been digitised or can be digitised regardless of the fact that digitisation is always a transcription and there can be no impartial transcription of the world and its events (what is "recorded" always depends on the location, the dissemination and the sensitivity of the sensors). "Raw data" themselves are the result of a sophisticated process of de-indexation, decontextualisation and removal of anything that could relate a piece of data to what makes a life special or different.

data processing significantly affecting data subjects, taking account of specific circumstances of the persons in question. In particular, if it is suspected that there has been indirect discrimination as a result of the involvement of automated data processing in the decision-making process or because of an obvious – and not easily overcome – lack of transparency of the processing methods involved (including self-learning and machine-learning systems), the burden of the proof that there have been no discriminatory effects should be shifted to the persons making use of automatic systems to take their decisions. This reversal of the burden of proof is entirely in keeping with the requirement imposed on controllers by **Article 8bis2**, which is to design data processing in such a manner as to prevent or minimise the risk of interference with rights and fundamental freedoms.[82]

This solution, however, comes up against the uncertainties that still surround the applicability to relationships between individuals of Article 14 of the European Convention on Human Rights prohibiting discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. Although there is no theoretical obstacle to acknowledging that Article 14 of the Convention has a horizontal effect,[83] the possibility that the responsibility of states may be incurred because of their inaction when cases of discrimination occur between private persons still depends on the interpretation of the European Court.

If this uncertainty could be dispelled, the following steps should be taken:

- Article 8 c. should be reworded as follows: "c. to obtain, on request, knowledge of the reasons given, in view of his or her specific circumstances, for the decision taken on the basis of automated data processing."
- The following sentence should be added at the end of Article 8bis2: "In particular, all Parties shall ensure that controllers and recipients demonstrate to the relevant supervisory authority that decisions taken on the basis of automated data processing do not have discriminatory effects that are incompatible with the right to equal opportunities following from Article 14 of the European Convention on Human Rights".

- *"Every individual shall have a right to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her" (**Article 8.c**)*

In the context of decisions taken on the basis of Big Data-type processing, especially when they involve self-learning algorithms (see p. 12 above), the requirement that data subjects should be provided with "knowledge of the reasoning underlying data processing" is both unrealistic and deeply paradoxical.

It is unrealistic in so far as, possibly by definition, algorithms (particularly self-learning ones) operate in accordance with inductive processes which, as they do not involve theories or hypotheses, cannot be easily communicated or are not intelligible to human beings. These processes cannot be readily translated into any narrative form. In the case of unsupervised

[82] Article 14 of the European Convention on Human Rights states expressly that "the enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status".

[83] See Picheral C., "Discrimination raciale et Convention européenne des Droits de l'Homme (l'apport de la jurisprudence)", *Rev. trim. dr. h.*, 2001, pp. 517-539.

algorithms, they may not actually even be “logical processes”, but “insights” of the algorithm, which identifies models or patterns among relatively unstructured masses of data, depending in particular on priorities linked to the need to optimise its own functioning. And what algorithms “see” is not visible to us. We can experience the effects when decisions are taken on the basis of the “algorithmic insight” but we cannot explain the process which governs the identification by the algorithm of the correlations liable to form themselves into a model.

This requirement to communicate the “reasoning underlying data processing” is also paradoxical in that, as David Golumbia explains, “computational, mechanical, informatic, physical ‘perception’ of processes and objects takes place at all time, without reference to us and in modalities we cannot see, register or necessarily understand. Demanding that we be able to see something that is at the same time invisible to and unrelated to human being and human perception is a clear paradox that demands both *a* and *not-a* be true at once.”[84]

Whereas the requirement for the “reasoning”[85] underlying data processing to be communicated when the results of this processing are applied in a decision taken with regard to a person is liable to improve the situation of data subjects by ensuring at least that there is some symmetry between the information provided to them and to the controller or recipient, this requirement is unrealistic and insurmountably paradoxical in a Big Data context.

Lastly, even if it were possible to communicate to individuals the “reasoning” underlying data processing, this would in no way be sufficient, without also making transparent and communicable the origin and nature of the processed data, the characteristics of the data sensors or recording instruments and the “cleaning” processes of these data, whereas one of the characteristics of Big Data is to ignore their context of origin and the material conditions under which they were produced.

In this context, it seems to us that a more important safeguard against the excessive use of algorithms in decision-making processes than a requirement for transparency which cannot be achieved by the processing system concerned is the requirement for reasons to be given for the decision in the light of the data subject’s specific circumstances (which should not be reduced to the “profile” produced by the algorithm) (see p. 42). This requirement for specific reasons ensures that decisions can be challenged and forces the persons taking such decisions to take responsibility for them.

3 CONCLUSIONS

Today, we find that digital data plays an increasingly predominant role in informing and guiding action, in virtually all sectors of business and government. Personal or anonymous data are the new social modelling co-ordinates. It is on the basis of these data rather than on the basis of institutional or deliberative processes that the categories, by means of which individuals are classified, evaluated, rewarded or punished, are drawn up. These same categories are used to evaluate the merits and needs of individuals or the opportunities or dangers underlying the lives they lead. In this view of “government by data”, how can we ensure the survival of individuals as subjects of law? How can we ensure that individuals are not viewed only as temporary digital data aggregates exploitable en masse on an industrial scale but as subjects of law in their own right.

[84] Golumbia D., “Judging like a Machine”, in. Berry, D. M., Dieter M. (eds.), *Postdigital Aesthetics: Art, Computation and Design*, Palgrave Macmillan, 2015.

[85] It is not certain that these algorithmic processes, when becoming self-learning, can still be regarded as “reasoning” if by that we imply an *a posteriori* synthetic judgment dimension

The processes of personalisation and profiling (at the expense of approaches using pre-existing categories) specific to the governmentality of the Big Data world make this fundamentally different from the hypotheses of "bio-power" described by Michel Foucault – a power whose purpose is to "exert a positive influence on life, that endeavours to administer, optimise and multiply it",[86] and "whose major role is to ensure, sustain, optimise and multiply life"[87] – and of the "biopolitics of populations" – which appears to have emerged in the second half of the 18th century targeting human diversity as "a global mass that is affected by overall processes specific to life, such as birth, death, production, illness".[88] Clearly, moreover, algorithmic governmentality shares certain features with bio-power and biopolitics, such as the fact of relying decisively on statistical practices. Life itself – the life of individuals as individual bodies and psyches, and the life of populations as being affected by overall processes specific to life – seems strangely deserted in favour of a digital environment which increasingly cuts itself off from the outside: as if what needed to be "governed today" was not so much individuals in flesh and blood, capable of suffering and addressed as beings subject to rights and obligations, having to account for their acts and decisions, but networks of aggregated data in the form of "predictive" models, embodying nothing other than pure potentiality, economic expediency detected in real time, i.e. pure expediency, finalised only in terms of the acceleration and objectification of decision-making processes themselves, i.e. ultimately the automisation of decisions.

Individuals, fragmented as they are in the form of a myriad of data relating them to a multitude of profiles (consumers, potential fraudsters, employees of varying degrees of reliability and productivity, etc.) all of which apply only to them as individuals, without being considered in any collective context (unlike the traditional models of categorisation such as ethnic profiling, adjusted in line with socially proven classifications which could therefore result in collective action), and no longer obliged to account for themselves, become infinitely calculable, comparable, indexable, interchangeable and in competition – an absolute competition which is no longer limited by or linked to any standard (of merit, desirability, need, equity, etc.) – with all others on a quasi-molecular scale in a system based on reputation, risk and opportunity (rather than on accomplishments) operating in an automated way at the subliminal level of infra-personal data. We in the 21st century like to think of ourselves as constantly evolving, unfinished and only partially defined processes, open to new possibilities which this lack of definition makes possible rather than completed beings assigned once and for all into a social status, profession or category – which is why we insist on securing through law, in particular through the right to protection of privacy, a "freedom from unreasonable constraints on the construction of one's own identity".[89] But we also wish to protect ourselves against the "horror of having neither shadow nor reflection, of being reduced to an absolutely blank existence which has become porous and devoid of substance (…) the terror of being freed of the burden of our inner shadow, of this nebulous velvety lining for our inner and outer beings".[90] Clément Rosset commented that the French word "personne" means both somebody and nobody "an echo of the original link which binds the definite to the indefinite, the something to anything, the presence of one thousand paths to the absence of any path". [91] This double meaning of the word "personne" betrays a powerful ambivalence, in the very heart of subjectivity, in respect of the very principle of subjectivation processes: as an evolving presence, a person cannot be

[86] Foucault M., *The history of sexuality, Vol. I, The will to knowledge*, Allen Lane, 1978.
[87] *Ibid.*
[88] Foucault M., "*Society must be defended". Lectures at the Collège de France, 1975-1976*, Allen Lane, 2003.
[89] Agre P. E., Rotenberg M. (eds.), *Technology and Privacy. The New Landscape*, MIT Press, 1998, p. 7.
[90] Foucault M., *L'usage de la parole: deuxième série: langages de la folie: 4 – Le corps et ses doubles,* 28 January 1963.
[91] Rosset C., *Le Réel. Traité de l'idiotie,* Minuit 1977/2004, pp. 18-19.

defined once and for all. In the Big Data universe, through the remote objectivity of "predictive" profiling, it is in their two-fold dimension of presence and absence, in their paradox or their constitutive "fold"[92] that individuals are side-lined.

The legal systems for protecting individuals with regard to automatic processing of data must therefore, first of all, ensure that individuals, subjects of law, have a presence, an impact, a consistency in a universe in which only temporary data aggregates exploitable en masse on an industrial scale count. Secondly, they must prevent people being locked into "categories" or "profiles" they know nothing about and which they are unable to challenge. Giving consistency to subjects of law does not mean "putting consumers at the centre" by surrounding them with the means of detecting what they might be interested in purchasing, even before they themselves have given the matter any thought or expressed any intention, nor is it pre-emptively regarding as definite, behaviour that is only potential (and the potentiality of which is established by nothing other than algorithmic modelling), but rather always taking into account individuals' capacity for not doing or wanting everything which they are "statistically" predisposed to do or want, and to always assert their right to themselves account for their own motivations. Subjects are shown no respect if we do not at the same time respect their capacity for reticence, for reservation, for not doing what the algorithms predict and their ability to say, for themselves, what prompts them to act.

The above considerations therefore implicitly advocate a renewed focus on and protection through law of these two essential "attributes" of subjects of law. What we therefore need to guarantee, as "meta-rights" or the capacities that are necessarily recognised and protected under the rule of law is:[93]

1) the faculty to disobey, not always to be where we are expected to be, not to do everything we are capable of according to algorithmic projections;

2) the responsibility to ourselves account for our own actions, decisions and intentions in spite of algorithmic recommendations and profiling.

Therefore what the foregoing considerations invite us to do is to relocate the gravitational centre of legal subjectivity and protect it by law, focusing not so much on people's capacities of understanding and volition, or their control over their intentions, but on a certain inclination towards spontaneity and unpredictability, an open-minded approach to events and an ability to express ideas, however far-fetched. It is only by reframing the concept of "subjects of law" in this way that it is possible to imagine how applications based on data intelligence can be developed in harmony with the mutually supportive, political beings that we are. Furthermore, and almost by definition might one say, it would be impossible to cover the whole subject of Big Data and the ethical, legal and political challenges posed by the "digital turn". Accordingly, this "digital revolution" calls for constant vigilance and a continually renewed examination of the relevance and appropriateness of the legal instruments for protecting our fundamental rights and freedoms.

[92] I refer, of course, to the "fold" described by Gilles Deleuze (Deleuze G., *The Fold, Leibniz and the Baroque*, University of Minnesota Press, 1993).

[93] On the subject of "meta-rights", by which we mean a series of individual faculties or prerogatives which are necessarily entailed by the rule of law and make it possible for rules to be debated and challenged, please refer to Rouvroy A. and Berns T., "Le nouveau pouvoir statistique – Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps 'numériques'", *Multitudes*, 2010/1 No. 40, pp. 88-103.