Comparative Law Review

VOLUME 11/2

ISSN: 2038-8993

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Department of Law - University of Perugia
Via Pascoli, 33 - 06123 Perugia (PG) - Telephone 075.5852437
Email: complawreview@gmail.com

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.

COMPARATIVE
LAW
REVIEW
VOL. 11 /2

Remembering Stefano Rodotà

[±]OF MACHINES AND MEN. THE ROAD TO IDENTITY
SCENES FOR A DISCUSSION[*]

Stefano Rodotà

1.In the reflections on the "homme-machine" by La Mettrie and D'Holbach[1], the physical and psychical identity is ordered, in a regulatory sense, by nature. But it is the relationship with the world of machines that shows that identity is a complex social entity, irreducible solely to naturalistic data, resulting from a never accomplished historical event. Montaigne reminds us that life, in which identity is reflected, "est un mouvement inégal, irrégulier, multiforme"[2], thus a continuous construction, entrusted to variable contexts, departing from any automatism. Furthermore, if the order that governs identity were only naturalistic, then the autonomy of a person itself would be denied at its origin.

Rather, throughout history we have always tried to force the limits of nature, especially when we have tried to mimic it, reproduce it, transport it to a different dimension. It is not a paradoxical conclusion, but just when reproduction of nature appears at its zenith, the highest degree of artificiality has been reached. The automatons, the Ingenious Devices have fascinated us since ancient times; they have paved the way to other mechanical creatures, like robots and the different thinking machines; and then came the cyborgs, announcing the trans- and post-human, the researches on brain-machine interfaces (BMIs) or brain-computer interfaces (BCIs). But relations between man and the world of machines are not linear[3]. The fact that we start from man as a reference or model may lead to very different results: to try to replicate man in a machine or to replicate machine in a man, an object among other objects, in fact an "homme-machine".

[±] The editorial team of the Comparative Law Review has decided to publish this contribution of Professor Stefano Rodotà to celebrate him on the Fifth anniversary of his passing. Both papers engage with new technology, identity, data and legal rules. It seems the best way to remind how important his work is within the academia.

[*] The title of this paper mimics that one of a well known John Steinbeck's novel, "Of Mice and Men" (1937), a story of an unconscious destructive power that can be stopped only through the destruction of that power itself. Violence, public or hidden, against violence? We must avoid any aggressive attitude. To mimic William Shakespeare (King Lear, act V, scene II, "Ripeness is all") we could say "Consciousness is all".

[1] J. 0. de La Mettrie, L'homme machine (1748), in Oevres philosophiques, 2 vol., Fayard, Paris, 1987; P. H. T. D'Holbach, Svg}jeipe de la nature (1770), 2 vol., Fayard, Paris, 1990.

[2] M. de Montaigne, Essais (1588), Livre III, chap. III, De mois commerces.

[3] M. G. Losano, Storie di automi. Dall'antica Grecia alla belle époque. Einaudi, Torino 1990; C. Sini, L'uomo. la ma«china l'automa, Bollati Boringhieri, Torino 2009.

Social concern has always accompanied these matters; it has brought about many reactions against, and radical criticism of, mechanicism; the most well known and extreme reaction was the one that went under the name of Luddism, which manifested itself still in the '60s when Harvey Matusow and his International Society for the Abolition of Data Processing Machines demonstrated in front of the IBM offices, raising banners saying: "Computers Are Obscene". Criticism of technological progress has expressed itself in various forms, to protect man from a fate that makes him become "a happy slave of machines" and to prevent the whole of society from changing into a relentless control machine.

In reality, great dystopias and utopias constitute an essential cultural background at the basis of any discussion on the man-machine relationships. Turnarounds are continuous. It is the progressive integration with the world of science and machines, in fact, that has been considered also as an extraordinary chance given to the world of humans to reach a fullness that it had lacked till then.

The *Magnalia naturae* listed by Francis Bacon at the end of New Atlantis[4] comes back to the mind: "the prolongation of life; the retardation of age; the curing of diseases counted incurable; the mitigation of pain; the altering of temperament, the statures, the physical characteristics; the increasing and exalting of the intellectual parts; versions of bodies into other bodies; making of new species; drawing of new foods out of substances not now in use".

All this, today, can also be considered in the dimension of rights, a construction of identity that ends up coinciding with the construction itself of humans. After the Oskar Pistorius issue, the South African runner running with two carbon fibre artificial limbs replacing his lower legs (authorised to participate into the Olympic Games), another paraolympic athlete, Aimée Mullins, said that "to change one's body through technology is not an advantage, but a right. Both for those doing sports professionally and common people". Thus the barrier between "normal people" and those with artificial prosthesis falls, and in fact a wider notion of "normal" is developed, which becomes a condition to freely construct one's identity using all the socially available opportunities. The new dimension of humans calls for a different legal measure, that can dilate the scope of the fundamental human rights.

Through the body people can take possession of technology, bringing it back to the dimension of humans. But what happens when these phenomena do not manifest

[4] F. Bacon, New Atlantis (published in 1627).

themselves as appropriation, but as expropriation, when people find themselves living in an environment where machines can take over their identity, change their body to enable its external control, when we live in an *augmented reality, ambient intelligence, ubiquitous* or *pervasive computing, smart environments,* when, all said and done, we live in an environment where machines can take on a position of supremacy, for whatever use is made of them or for their own autonomic nature?

2. To try and answer these questions, and grasp the new way in which identity is constructed, we have to start from the realisation that a social and legal order of machines is developing that claims its own autonomy, that not only may clash with people's traditional autonomy but also give rise to a new anthropology. Two judgements of the Bundesverfassungsgericht (the German Constitutional Court) may help clarify some aspects of the problem.

The first (15 February 2006) concerns par. 14.III of Luftsicherheitgesetz, that authorised military aviation to shoot down a civilian plane as, after having been hijacked by terrorists, it was feared that it could be used as a weapon against civilian or military targets (the case of the 9/11 attack to the Twin Towers and the Pentagon), without there being any other way of preventing such an outcome. The said rule was considered in contravention with Articles 1 and 2 of the Grundgesetz, on the dignity and defence of life, two particularly significant grounds. The german constitutional judges, in fact, thought that the passengers of the aeroplane were being "depersonalised and, at the same time, deprived of their rights" ("verdinglich und zugleich entrechtlicht"). A unilateral decision by the State on the life of the passengers deprived them of the right of every human being to autonomously decide of its own existence They were reduced to inanimate objects, to mere components of the plane, to be absorbed by the machine and undergoing a radical change in their prerogatives, in their 'human' status.

Just as important is the subsequent judgement of 27 February 2008, by which the Bundesverfassungsgericht declared in contravention with the Grundgesetz an amendment to the law about the domestic intelligence service of the Land North-Rhine Westphalia. The amendment had introduced a right for the intelligence service to "covertly observe and otherwise reconnoiter the Internet, especially the covert participation in its communication devices and the search for these, as well as the clandestine access to information-technological systems among others by technical means". The decision of the Bundesverfassunsgericht is widely considered a landmark ruling, because it constitutes a new "basic right to the confidentiality and integrity of information- technological systems" as part of the general personality rights in the German constitution. The reasoning goes: “From the relevance of the use of information-technological systems for the expression of personality (Persönlichkeitsentfaltung) and from the dangers for personality that are connected to this use follows a need for protection that is significant for basic rights. The individual is depending upon the state respecting the justifiable expectations for the integrity and confidentiality of such systems with a view to the unrestricted expression of personality.” (margin number 181). The decision complements earlier landmark privacy rulings by the Constitutional Court that had introduced the “right to informational self-determination” (1983) and the right to the “absolute protection of the core area of the private conduct of life” (2004).

Information-technical systems that are protected under the new basic right are all systems that “alone or in their technical interconnectedness can contain personal data of the affected person in a scope and multiplicity such that access to the system makes it possible to get insight into relevant parts of the conduct of life of a person or even gather a meaningful picture of the personality” (margin number 203). This includes laptops, PDAs and mobile phones.

The decision also gives very strict exceptions for breaking this basic right. Only if there are “factual indications for a concrète danger” in a specific case for the life, body and freedom of persons or for the foundations of the state or the existence of humans, govemment agencies may use thèse measures after approval by a judge. They do not, however, need a sufficient probability that the danger will materialize in the near future. Online searches can therefore not be used for normal criminal investigations or general intelligence work.

Let us compare this approach with the one that emerges from the front cover of the first issue of the 2007 Time's magazine, dedicated as is tradition to “the person of the year”, which spelled out in big letters the word “You”. Thus it was the endless numbers of individuals to be indicated as the protagonist. Each one, though, in their unrepeatable individuality, because the front page was made of reflecting material that allowed anyone looking at it to recognise himself as in a mirror. You are the world.

But, at a closer look, that mirror was a computer screen drawn over the word “You”. The message thus takes on a particular meaning. I recognise you as the person of the year because you have become part of the most significant technological apparatus. The man-machine order is upside down. You are a protagonist, and maybe the lord of the environment around you, only if you become a machine yourself, basically if you become a part of the apparatus.

In the German judgement of 2008 this approach is completely overturned. It is the human that embodies the machine, not the opposite. It is recognised that between man and machines not only is there an interaction, but a compenetration. This is a structurally evident data, and its constitutional relevance is recognised. The law thus reiterates the priority of humans, but manifests its power telling us that the world is going through a new entity, made up of the person and the technical apparatus to which data is entrusted. A continuum is established between the person and the machine: by recognising this, the law hands us a new anthropology, affecting legal classifications and changing their quality. Confidentiality, a quality of humans, is handed over to the machine.

It is not possible, then, to consider this judgement as just a further development of the orientation adopted by the Constitutional Court itself in 1983. By that historic judgement, the Constitutional Court recognised "informative self-determination" as a fundamental right, and radically changed the traditional picture of privacy protection, retrieving the more important indications of the cultural development started in the early '70s. In the 2008 judgement reference to confidentiality still appears, even if its transfer from the person to the machine already confirms a new approach. But two fundamental questions differentiate it from the previous ruling. The first concerns the fact that the notion of confidentiality is extended to comprise an ensemble that prevents reducing the person, and thus the human, to a mere material entity. From here, and this is the second important point, there is a new form of protection, that overcomes the dychotomy between *habeas corpus,* linked to the physical body, and *habeas data,* conceived as an extension of that historical protection of the electronic body. We no longer have separate entities to be protected but only one: the person in its different configurations, progressively determined by his relation with technologies, which are not only electronic.

We are facing the reconstruction of the integrality of the person, similar to the one realised through the recognition of a unitary protection of the person's integrity, no longer limited only to a physical integrity, but extended to comprise also psychical and social integrity, as explicitly set forth in the definition of health developed by the World Health Organisation ("a state of complete physical, mental and social well-being and not merely absence of disease or infirmity") and then transposed in a multitude of legal documents (e.g. Article 3 of the Charter of Fundamental Rights of the European Union). We could say, with some rhetoric emphasis, that the law, after having acknowledged the non-severability of the body and the soul, provides its version of “man machine” through the 2008 German judgement. Primary importance is given to human element, the only way to reconcile man with the technical apparatuses that progressively accompany, restructure and invade him. Personal identity is expanding. But who, concretely, is behind this? The answer emerging from the 2008 German judgement seems to tell us that it should always and only be the person concerned to set the conditions for defining his identity, by re-establishing his rule on a portion of the external world, and the technical apparatuses he directly uses.

That has never been the case, the construction of identity cannot be confused with the right to self—representation. But the technological changes in the methods for processing personal information have progressively changed the relationship between the identity freely constructed by the individual and the intervention of third parties, giving growing weight to the activities of the last mentioned.

Inaccuracies and partial representations, or even real falsifications, are a constant feature of many biographies freely developed by entities other than the person concerned, which then become part of the socially accredited information structures (like Wikipedia). Nowadays we also have “dispersed” identity, in the sense that information concerning the same person is entered in different data banks, each one of which only returns a part or a fragment of the overall identity. We risk entering a time of identity “unknown” to the person concerned himself, in the sense that not only is it found in different places, but also in places that are difficult or impossible to know of, or to have access to.

Our identity, thus, is more and more the result of an operation prevailingly conducted, processed and controlled by others. And we are not speaking here only of a construction based on the way the others see us and define us: “le Juif dépend de l'opinion pour sa profession, ses droits et sa vie”[5]Collective representation can determine the way in which we are considered, without necessarily providing the identity constitutive materials, as it happens when personal data is used directly. Furthermore, it is also true that in the one or the other case we have an “unstable” identity, at the mercy, from time to time, of moods, prejudices or the concrete interest of the entities collecting, storing and disseminating personal data. A circumstance of dependence is thus created that causes the construction of an “external” identity, and the classification of identity in forms that reduce the identity managing power of the person concerned.

[5] J.-P. Sartre, Réflexions sur la question juive, Gallimard, Paris, 1954, p. 106.

3. A small American story can help us understand a change that has already become a part of our daily lives. In a primary school of California, for security reasons, it was decided that each child would carry a necklace including a smart tag - a remotely readable RFID chip - to enable charting all his/her movements and localise him or her at any time. Back home, a little girl commented the novelty like this with her parents: "I do not want to become a packet of cereals". The reference made here is clear. It reflects the experience of a girl who, in a supermarket, sees that the things she buys are "read" by an electronic instrument through the bar codes, and refuses to be assimilated to a mere remotely readable object.

The little girl has understood everything, she has described a ehange that affects not only society, but the very anthropological nature of individuals. The body is giowing in its importance, and is changing its functions. lt is becoming a source of new information and is exploited by unrelenting data mining activities - it is a veritable open-air mine from which data can be extracted uninterruptedly. The body as such is becoming a password—physicality in replacing abstract passwords. Fingerprints, hand/finger/ear geometry, iris, retina, face scans, body odours, voice, signature, keystroke dynamics, gait recognition, DNA are increasingly used as biometric information not only to identify individuals or allow access to several servlces. but also to set up permanent categories and perf'orm additional controls following identification or authentication/verification, i.e. confirmation of someone's identity.

The body is getting into focus. A manipulated body is being created, which is primed towards surveillance and can be located. Technology is working directly on the body, Surveillance is no longef implemented from the outside, for instance by means of video surveillance. It is not enough to exploit physical features, as is the case with the use of biometric data. Indeed. the body is coupled Cth electronic devices - first and foremost, these based on the RFID technology. The body is supplemented and modified by means of the insertion of electronic implants and of the use of nanotechnologies. The body is being transformed as a whole, not only because it is becoming post- human or trans-human, but because the very autonomy of individuals is being affected - since individuals can be monitored and directed remotely. The body is therefore becoming a new object, wh‹ch also requires considering anew what is a personal data nowadays in order to ensure that the protection of such data as currently envisaged remains workable. and personal identity can remain nder control by the subject itself..

We have concrete examples before us. and they are growing in number by the day. We all are aware of the cases of employees required to carry a small "wearable computer", which allows the employer to guide their activities via satellite, direct them to the goods to collect, specify the routes to be followed or the work to be done, monitor all their movements and thereby locate them at all times. In a report published in 2005 by Professor Michael Blackmore from Durham University, commissioned by the English GMB trade union, it was pointed out that this system already concCmed thousand people and had transformed workplaces into battery farms" by setting the stage for *prison surveillance". We are facing a small-scale Panopticon, the harbinger of the possibility for these types of social surveillance to become increasingly widespread, Similar results, although concerning only location at the workplace, are already possible by means of the insertion of a RFID chip *in* employees' badges.

Some companies, like City Watcher in Ohio, took another step forward in the direction of manipulating its employees' bodies by requiring some of them to have a microchip implanted in their shoiitdefs in order to be idenlified at the entralice of restricted access areas. Thus, the body is modified in its very physicality and primed in order to be monitored directly. And the body implants pf remotely readable microchips are being increasingly used in the most diverse sectors. from disco clubs to hospitals, to open the door of one's house or start up one's computer - With a resulting cost reduction and growing ease of deployment exclusively in order to safeguard the data subjects' health. Any other utilisation should be regarded as in conflict with human dignity, which was declared inviolable in Article 1 of the Charter of fundamental rights of the EU, as well as with data protection principles.

What would be of a society in which a growing number of individuals were tagged and tracked? Social surveillance is committed to a sort of electronic leash. The human body is equated to any moving object, which can be monitored remotely via satellite technologies or else radiofrequency devices. If the body can become a password, location technologies are bringing about the creation of a networked person.

We are confronted with changes that have to do with the anthropological features of individuals. We are confronted with a stepwise progression: from being "scrutinised" by means of video surveillance and biometric technologies, individuals can be "modified" via the insertion of chips or "smart" tags in a context that is increasingly turning us precisely into "networked persons" - persons who are permanently on the net, configured little by little in order to transmit and receive signals that allow tracking and profiling movements, habits, contacts, and thereby modify the meaning and contents of individuals' autonomy. Technological drifts are therefore taking on especially disquieting features. The purposes of identification, verification, surveillance, security in transactions may they really justify any use of the human body that is made possible by technological evolution?

These considerations obviously also apply to the cases in which RFID technologies do not result into modifying a person's physicality. To address these issues, one should draw a distinction between the cases in which RFID tags are used as devices directly connected with a given individual (e.g. when they are embedded in an ID card), and the cases in which this link is brought about by the relationships with objects that are, in turn, tagged. In the former case, one has unquestionably to do with situations that are quite similar to those described in respect of body implants, although here the individual has always the option available to get separated from the medium containing the tag and thus escape surveillance - which is unfeasible, or actually much more difficult to do with regard to body implants, including reversible implants. In the latter case, it is necessary to adjust the current legislation on personal data protection by taking account of the pervasive nature of the control and classification this kind of data collection makes possible - as aptly pointed out in a Working Document adopted by the European Working Party on Data Protection. This implies, on the one hand, the need for re-considering the definition of personal data in order to counter the dangerous trend towards the adoption of formalistic and reductionistic interpretations, which may be prejudicial to the concrete protection of individuals exactly with regard to the applications of RFID technology - and not only this technology. On the other hand, one should seriously take into consideration the risk that standardisation, by allowing access to the data contained in the chip by a plurality of entities and enabling active interventions on such data, might result into controlling and manipulating identity.

This trend was explicitly confirmed by a declaration of the Prime Minister of the United Kingdom on 19 July 2004 to tag and track the five-thousand more dangerous English offenders via satellite. The technical difficulties involved in this project have been stressed by many, but it is the symbolic strength of the message that has to be seriously taken into consideration.

Basically it implies a deep change in the legal and social status of a person. The fact of having entirely served the sentence will no longer be enough to be free again. If it is considered as highly probable that a person will commit offences, then that person will loose his freedom of movement and all the relevant forms of individual autonomy, because he will be forced to have an electronic instrument attached to him that will make his location possible at an time. And this tagging of dangerous people can be achieved by putting a microchip under the skin. This would change the nature itself of the body, as by being technologically manipulated it becomes post-human. But canthis prospect be considered as compatible with the principle of dignity, which is set forth at the beginning of the Charter of Fundamental Rights of the European Union? Can we accept the Blairian semantic daring move that re-baptized this further version of the "society of surveillance" as "the society of respect"? In conclusion: we cannot accept that, networking people, our societies are turned into surveillance, selection, sorting societies; and that via networking and mass control free countries are turned into nation of suspects.

4. Thus, identity is built up in a scenario where one is increasingly dependent on the outer world — on the manner in which the surrounding environment is built up. One is dependent on other individuals as well as on the things surrounding them or else used to directly change their own bodies. In fact, we are living a true identity revolution, "the identity (...) is in the middle of a period of extraordinary tumult[6] in the age of the Web 2.0, of the coming Web 3.0, of the massive profiling, of the new dimensions of the cloud computing and of the autonomic computing. Two changes should be highlighted especially, both being related precisely to the Web 2.0 and 3.0.

Internet 2.0 has become an essential tool for a mass process of socialization and for the free development of the individual personality. In this perspective, the rights of expression are an essential part of the construction of the person and of its place in the society. The construction of one's identity is becoming increasingly a means to communicate with the rest of the world — to present one's self on the world's stage. This is changing the relationship between public and private sphere, indeed the very concept of privacy.[7]

Privacy has been conceived as an "exclusion" device — as a tool to fend off the "unwanted gaze". However, by analyzing the definitions of privacy one can appreciate how privacy has changed over time by giving shape ultimately to a right that is increasingly geared towards enabling the free construction of one's personality — the autonomous building up of one's identity, and the projection of fundamental democratic principles into the private sphere. The initial definition of privacy as the "right to be let alone" has not been

[6] J. D. Lasica, Identity in the Age of Cloud Computinq – The next generation of Internet's impact on business, governace and social interaction, The Aspen Institute, Washington D. C. 2009, p. 1.

[7] S. Warren-L. D. Brandeis, "The Right to Privacy", Harvard Law Review, l890,p. 4 ss.

done away with; rather, it is now part of a context that has grown out of different contributions. The first real innovation was brought about by Alan Westin, who defined privacy as the right to control how others use the information concerning myself.[8] Later on, privacy was also regarded as "the protection of life choices against any form of public control and social stigma"[9] as vindication of the boundaries protecting each person's right not to be simplified, objectified, and evaluated out of context"[10] and more directly as "the freedom from unreasonable constraints on the construction of one's own identity[11]. Since the information flows do not simply contain "outbound" data - to be kept off others' hands - but also "inbound" information - on which one might wish to exercise a "right not to know" - privacy is also to be considered as "the right to keep control over one's own information and determine the manner of building up one's own private sphere"[12] and as "the right to freely choose one's life[13].

In 2000, the Charter of Fundamental Rights of the EU recognized data protection as an autonomous right. This can be considered the final point of a long evolution, separating privacy and data protection. The evolution is clearly visible by comparing the EU Charter with the provisions made in the 1950 Convention of the Council of Europe. Under Article 8 of the Convention, "everyone has the right to respect for his private and family life, his home and his correspondence". Conversely, the Charter draws a distinction between the conventional "right to respect for his or her private and family life" (art. 7), which is modelled after the Convention, and "the right to the protection of personal data" (art. 8), which becomes thereby a new, autonomous fundamental right. Moreover, article 8 lays down data processing criteria, expressly envisages access rights, and provides that "compliance with these rules shall be subject to control by an independent authority".

The distinction between right to respect for one's private and family life and right to the protection of personal data is more than an empty box. The right to respect for one's private and family life mirrors, first and foremost, an individualistic component: this power basically consists in preventing others from interfering with one's private and family life.

[8] A. Westin, Privacv and Freedom. Atheneum, New York, 1970.

[9] L. M. Friedman, The Republic of Choice. Law. Authority and Culture, Harvard U. P., Cambridge (Mass.), 1990, p. 184.

[10] J. Rosen, The Unwanted Gaze. The Destruction of Privacv in America.. Random House, New York,2000, p. 20.

[11] P. E. Agree-M. Rotenberg, Technology and Privacv. The New Landscape, Mit Press, Cambridge (Mass.), 2001, p. 7.

[12] S. Rodotà, Tecnoloeie e diritti, Il Mulino, Bologna 1995, p. 122.

[13] F. Rigaux, La protection de la vie nrivée et des autres biens de la tiersonnalité, Bruylant, Bruxelles-Paris, 1990, p.167.

In other words, it is a static, negative kind of protection. Conversely, data protection sets out rules on the mechanisms to process data and empowers one to take steps — i.e., it is a dynamic kind of protection, which follows a data in all its movements. Additionally, oversight and other powers are not only conferred on the persons concerned (the data subjects), as they are also committed to an independent authority (Article 8.3). Protection is no longer left to data subjects, given that there is a public body that is permanently responsible for it. Thus, it is a redistribution of social and legal powers that is taking shape. It is actually the endpoint of a long evolutionary process experienced by the privacy concept — from its original definition as right to be left alone, up to the right to keep control over one's information and determine how one's private sphere is to be built up.

Furthermore, article 8 should be put in the broader context of the Charter, which refers to the new rights arising out of scientific and technological innovation. Article 3 deals with the "right to the integrity of the person", i.e. the protection of the physical body; Article 8 deals with data protection, i.e. the electronic body. These provisions are directly related to human dignity, which article 1 of the Charter declares to be inviolable, as well as to the statement made in the Preamble to the Charter— whereby the Union "places the person at the heart of its activities". Thus, data protection contributes to the "constitutionalisation of the person" — which can be regarded as one of the most significant achievements not only of the Charter. We are faced with the true re-invention of data protection — not only because it is expressly considered an autonomous, fundamental right, but also because it has turned into an essential tool to freely develop one's personality. Data protection can be considered to sum up a bundle of rights that make up citizenship in the new millennium.

If one probes deeper into the layered safeguards applying to the various categories of personal data, one can appreciate a highly meaningful paradox: indeed, many of the so-called "sensitive data", especially those concerning opinions, are afforded strong safeguards not so much to better ensure that they are kept confidential, but to enable *public* disclosure of those data without running the risk of discrimination or social stigma. My political opinions or my religious beliefs go hand in hand with and make up my identity only to the extent I can place them outside my private sphere — to the extent I can make them public. The true focus of protection is equality rather than confidentiality.

If identity becomes a relational concept, data protection takes on a different meaning. Social networking, which is the flagship of Web 2.0, mirrors this change in perspective most clearly. You join Facebook because you want to be seen and get a permanent public identity that goes beyond the fifteen minutes of fame Andy Warhol considered to be everyone's right. You feed the "public" sphere to so that your "private" can make sense. You exhibit a set of personal data, your electronic body, exactly like one's physical body is exhibited via tattoos, piercing, and other identity sign[14]. Identity becomes communication. But what happens with this identity that is totally geared to the outer world? It becomes more readily available to data mining activities[15] - whereupon one might wonder whether social networking also entails an implied consent to the collection of networked data. Or should the principle of purpose specification apply further, whether directly or indirectly, in order to make such data collection legitimate? These questions re-surface if one considers Internet 3.0 — the Internet of Things — and autonomic computing in terms of their being new methods to create and collect personal data.

We are about to experience what an EU research group termed a "digital tsunami", which might ultimately overthrow the legal tools that safeguard not only the identity, but the very freedom of individuals[16]. We are faced with an in-depth change in societal organisation, whereby the public security criterion is liable to become the sole benchmark.

This objective is stated openly. A document by the EU Council Presidency reads as follows: "Every object the individual uses, every transaction they make and almost everywhere they go will create a detailed digital record. This will generate a wealth of information for public security organisations, and create huge opportunities for more effective and productive public security efforts". Furthermore, "in the near future most objects will generate streams of digital data (...) revealing patterns and social behaviours which public security professional can use to present or investigate incidents". A Statewatch report, The Shape of Thines to Come (the same title of a 1933 novel by H. G. Wells)[17] shows how the EU has substituted the concept that data relating to EU citizens should in principle be kept private from State agencies, in favour of the principle that the State should have access to every detail about our private lives. In this scenario, data protection and judicial scrutiny of police surveillance are perceived by the EU as "obstacles" to efficient law enforcement cooperation. This implies that European

[14] D. Le Breton, Signes d'identité. TJtotiRces. piercines et autres marques corporelles. Métailé Paris, 2002.

[15] M. Hildebtandt-S. Gutwirth (eds.), Profiling the European Citizen – Cross disciplinary perspectives, Berlin- Heidelberg, 2008;F. Giannotti-D. Pedreschi (eds.), Mobility. Data Mining and Privacy, Geographic knowledge Discovery, Berling-Heidelberg, 2008.

[16] EU Future Group, Freedom. Security, Privacx — European Home Affaire in an open world, 2008 https://www.statewatch.org/news/2008/september/eu-future-group-report-freedom-security-privacy-european-home-affairs-in-an-open-world/

[17] T. Bunyan, The Shape of Things to Come. Statewtach, September 2008.

governments and EU policy-makers are pursuing unfettered powers to access and gather masses of personal data on the everyday life of everyone, on the ground that we can all be safe and secured from perceived "threats".

The criticisms by Statewatch are levelled against a specific feature of the digital tsunami — the growing use of the public security argument to downsize freedoms and rights and turn our societal organisation fiom a society of free individuals into a "nation of suspects". This is unquestionably a key issue because it has to do with the change in the relationship between citizens and State; more specifically, it is a violation of the undertaking made by the State vis-a-vis every individual that their data will be used selectively in compliance with such principles as data minimization, purpose specification, proportionality, and relevance. ia this manner, some of these principles underlying the system of personal data protection are being slowly eroded. This applies, first and foremost, to the purpose specification principle and the principle concerning separation between the data processed by public bodies and those processed by private entities. The only principle to be referred to becomes the principle of availability, with a view to improving the exchange and use by law enforcement agencies. The multi-functionality criterion is increasingly applied, at times under the pressure exerted by institutional agencies. Data collected for a given purpose are made available for different purposes, which are considered to be as important as those for which the collection had been undertaken. Data processed by a given agency are made available to different agencies. It means that individuals are more and more transparent and that public bodies are more and more out of any political and legal control. It implies a re distribution of political and social powers.

This means that the so-called digital tsunami should also be evaluated from different standpoints — starting exactly from the identity perspective. The full availability of all personal data to public agencies brings about a veritable transfer of identity into the hands of such agencies, which can actually rely on information that is unknown to the given data subject. This phenomenon is bound to take on increasing importance in view of the increasing amount of object-generated information. One comes face to face, in this manner, with one of the key features of data protection — the right of access, meaning everyone's unconditional power to know who holds what data concerning them and how such data is used. This can be the stepping stone to start re-constructing one's identity, by having any data that is untrue, obtained unlawfully and/or kept beyond the allotted time cancelled or erased; by having any data that is inaccurate rectified; and by supplementing any incomplete data. However, this has turned by now into a never-ending story — a bottomless chasm, because never does the recording of every trace we leave come to an end. "Know thyself' is no longer a precept that requires us to only probe into ourselves. Indeed, it relies on the assumption that one should manage to get back to different sources in order to establish not so much what the others know about us, but who we are in the electronic dimension — where a major portion of our lives are nowadays to be found.

We have to do with issues that relate to autonomy and the right to freely develop one's own personality. Everyone's freedom to know and build up their own selves is being increasingly constrained, whilst it is increasingly easier for others to become the lords and masters of our lives.

5. Thus, it is not enough to remark that we are living by now in a "networked public sphere", to quote Yochai Benkler[18]. It is necessary to consider how this public sphere is being created, by whom it is created, and how the public sphere in question is being shaped on account of these changes. The stepwise descent into a smart environment populated by intelligent things is giving rise to yet another shift, which goes beyond what has brought about the stepwise separation/opposition between one's self and the others as related to building up one's own identity. Indeed, there is a widening gap between individuals and machines due to the growing autonomy of the latter as mirrored by the so-called autonomic computing. The power to set the boundaries of human beings and their identity is increasingly shifted from the realm of man's appreciation to that of automated decisions.

An analysis of the above issues raises several questions. One can start from Article 15 of EU Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This article, at point (1), provides that "member States shall grant the right to every person not to be subject to a decision which produces legal effects regarding him or significantly affects hlm and which is based solely on automated process of data intended to evaluate certain personal aspects relating to him, such as performance at work, creditworthiness, reliability, etc.". For the sake of simplification, one might argue that this is a general provision on the allocation of decision-making powers in the digital world.

However, the symbolic as well as practical import of this provision is markedly reduced by the restrictive interpretation espoused by several domestic laws and, in particular, by the increasingly widespread, sophisticated application of profiling techniques — which

[18] Y. Benkler, The Wealth of Networks. How Social Production Trasforms Markets and Freedom. Yale University Press, New Haven, 2006.

have changed the very meaning of "decision". The studies on data mining and profiling have highlighted the basically regulatory importance attached to categorization, which is often socially more binding than legally binding decisions. This point is actually made in the EU directive, which refers to decisions "significantly affecting" persons. Profiling results into social sorting and accordingly brings about the risks of social stigma and exclusion. It is no chance that the definition of privacy had already emphasized the risk of social stigma well in advance of the coming of the age of profiling.

The creation of this new environment results into changes in individuals' behaviour; these changes have often been described and consist in self-restraint, "spontaneous" normalization, and the a priori adoption of mainstream behaviour. Profiling mirrors the modelling of society, which gives rise to mainstream behaviour rather than normalcy — which is actually no news to the scholars of cultural models, because the influence of such models is not a function of their formally binding value, but of their being regarded as a necessary step in view of social acceptance at the most diverse levels. This effect is enhanced further by data mining and profiling, because models are customised and linked to single individuals — ultimately, they are used in a targeted, selective manner. Social acceptance is shaped thereby as a kind of "compulsory" identity.

The possibility to escape from this mandatory scenario by relying on the system introduced by directive 95/46 is jeopardised further by the considerations put forward to criticise the view that exclusively automated decisions are unacceptable. It is argued that the human presence — considered to be a fundamental component of any legitimate decision-making — features from the start in this context: "humans will write the software, shape the database parameters and decide on the kinds of matches that count[19]. This argument is supported further by the consideration that automated decision-making processes are increasingly similar to human decision-making. It is no chance that the autonomic computing paradigm has been inspired by the human autonomic nervous system. "Its overarching goal is to realize computer and software system and applications that can manage themselves in accordance with high-level guidance from humans"[20] If what is artificial is increasingly modelled after nature, there is no longer any reason for the ban set

[19] P. M. Schwartz-R. D. Lee-I. Rubinstein, Data Mining and lnternet Profiling: Emerging Regulatoryand Technological Approaches, Berkeley Center for Law and Technology, Paper 50. 2008, p. 282.

[20] M. Parashar-S. Hariri, "Autonomic Computing: An Overview", in J.-P. Banatre et al. (eds.), UPP 2004, LNCS 3566, Springer, Berlin-Heidelberg, 2005, p. 247.

forth in article 15 of directive 95/46. The severance from the human factor is seemingly complete.

In the light of this blunt elimination of any boundaries between human and artificial processes, it should be pointed out that the staunchest supporters of the above stance are those who claim that markets and security should have the upper hand. Monitoring individuals and turning them into mere consumers are regarded as priority objectives that allow for the use of any tools. This impacts directly on identity, which is increasingly built up via external entities — and the interests vested in such entities may be completely different from those vested in the given individuals, who are deprived accordingly of any opportunity both for exercising their self-governance powers and for controlling who has got hold of their identities.

Can one re-appropriate at least some measure of control by relying, first and foremost, on the guidance set forth in directive 95/46? There are three points to be made in this connection. Firstly, it is necessary to uphold the principle whereby a wholly automated decision should never replace a decision that involves some sort of human involvement. Secondly, one should consider the access rights vested in every data subject under Article 12(a) of the directive, in particular with a view to knowing "the logic involved in any automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15(1)." The emphasis put on logic is especially important because it is linked to another key feature, i.e. the contribution given by technology designers[21] and the circumstance that digital technologies are built around their own "code"[22] which means that the control issue is also to be taken into account. Furthermore, since the limitations and constraints applying to subject access are widely known[23] - and this is the third point to be made — one should envisage access by collective entities acting on a data subject's instructions, which is already the case with some domestic laws. This solution — which is reminiscent of the approach that has emerged from the history of trade unions — would help reduce

the power unbalance of the individual stakeholders, bring about enhanced transparency, and above all initiate wide-ranging control processes based on societal self-organisation schemes.

[21] A. Rouvroy, "Privacy, Data Protection, and the Unprecedented Challenges of the Ambient Intelligence", Studies in Ethics, Law, and Technology, vol. 2, issue 1, 2008, p. 44.
[22] L. Lessig, Code and Other Laws of the Cyberspace, Basic Booke, New York, 1999.
[23] M. Hildebrandt, "Profiling and the Identity of the EuropeanCitizen", *supra* note 16, pp. 303-337.

In this perspective, four more issues must be taken into account. The first one looks at the "anonymity" (alias, pseudonym) and to the encryption as tools that make possible not to be identified and, consequently, not to be profiled, with a dichotomy between online persona and real- world identity.. The second looks to "the right to make silent the chip", immediately referred to the Rfid technologies, but that can be extended to the many devices making possible the multifarious forms of distance control (localisation and so on). The third underlies the necessity of "sunset rules" on data retention. The fourth is connected directly with cloud computing.

Cloud computing is a shorthand for defining a vast, always-on, accessible, broadband-enabled next-generation Internet. This new dimension must be looked at in connection with the changes of the online identity produced by the social Web. "Blogging became a mainstream activity, and with it came a different mind set. With a few exceptions, bloggers found the need to stand behind their words. They needed to tie their online musing to their real lives. Authenticity and transparency not imagination and anonymity — became the cardinal rules of the blogsphere[24]. This conclusion could be criticised, but it is true that with the rise of You Tube, of the video sharing sites, of the social networking sites such as MySpace and Facebook the situation has changed, and Facebook became the first Web service requiring validated identities, even if it not difficult to create false identities, becoming the largest platform of the cloud computing era. It implies that the personal data posted in Facebook need a fresh approach, because the traditional protection provided by the principle of the consent could not work, due to the fact that the posting is voluntary. Taking into account this novelty, it has been suggested to make reference to the purpose specification principle, so that the personal data made public for a merely social interaction with other people cannot be accessed and treated for different finalities (marketing, control).

The identity in the cloud has suggested a new approach to the identity itself in the social context, going toward a "user-centric open identity network". The idea is "an identity system that is scalable (so it works everywhere), user-centric (serving your interest, instead of something done to you by outside interests) and, importantly, customizable. This new system would recognize that each of us has multiple identities. We will be able to spoon out bits and pieces of our identity, depending on the social or business context we find ourselves in (...) You could separate your identity into discrete units and assign different

[24] J. D. Lasica, Identity, supra note 7, p. 16.

access permission depending on your role in a given situation. You could create a business profile, a health care profile, a friend profile, a mom or singles profile, a virtual profile and so on (...) Few identity softwar developers expect that most people want to manage their own identities[25]. Can we look at this suggestion as a road to the reconquest of individual power on identity?

6. Autonomic computing should be regarded in the perspective of this force field. It is a fact of life that should be understood in cultural terms and requires mechanisms of societal control, which need not rely on laws only. It is unquestionable that we are faced with the re-definition of the whole context applying to the relationship between identity and autonomy, which is bound to impact on the meaning and import of these two concepts. In fact, autonomic computing might mark the ultimate separation between autonomy and identity. Identity is becoming objective via mechanisms that do not rely on awareness of one's own self; it is turning into a functional replacement for autonomy — at least to the extent an adaptive scheme is built out of an identity that was "captured" at a given time, with all the respective features and needs, whereupon that identity is committed to self-management systems that can provide responses and meet the requirements arising out of the given circumstances. The construction of this "adaptive" identity might be regarded as a process that originates exactly from the freezing of that identity and keeps on adapting it to the relevant environment without any decisions being made and/or any awareness being developed by the individual. This is made possible by the unrelenting collection of information yielding statistical estimates that can accordingly anticipate/implement what the individual data subjects would have decided in the given circumstances. The possibility of a conscious interventions by the individuals could be totally excluded, making impossible their participation by default too. The construction of identity depends on algorithms, and we must be aware of the role played by mathematic models and algorithms as key elements of an economic organisation that has produced the financial crisis.

In fact, the environment can act upon the user's behalf without conscious mediation. It can extrapolate behavioural characteristics and generate pro-active responses[26]. One might argue that we are faced with the separation between identity and intentionality, which may give rise to unaccountability, discourage the propensity to change, and jeopardise a vigilant approach to the governance of one's self. Indeed, one should wonder whether the

[25] J. D. Lasica, Identity, supra note 7, pp. 17-18.

[26] E. Aarts-B. de Ruyter, "New research perspectives on Ambient Intelligence", in "Journal of Ambient Intelligence and Smart Environments", 2009, p. 8.

activities performed via autonomic computing are a projection from the past rather than the anticipation of future events[27].

7. Autonomic computing, which is not expressed solely by the specific functions described above, is setting the cultural, political and institutional agenda. It is bringing about an information collection mechanism that — as well as being wide-ranging and pervasive — 1s not static, but rather intrinsically dynamic. This means that it produces effects without any mediation being required, without having to make the information available to other entities or else use it for subsequent processing operations. Obviously, given the manner in which personal data are collected, opportunities also arise for such data to be used further, which increases not only the chances to automatically meet the given requirements, but also the overall transparency of individuals. And it means that, at same time, not only a new "inner" space of the person, but as "outer" space is currently being shaped.

Given this context, one is bound to turn once again to personal data protection seen not only as "a necessary utopia"[28], but also as a way to ensure the freedom of individuals and conditions for the democratic exercise of powers. Indeed, the technological changes impacting on social organisation do not only give rise to unbalances in the distribution and practice of power- They also bring about a societal gap between increasingly transparent individuals and increasingly opaque, unbridled powers.

Especially after 9/11, the boundless collection of personal data has been used as an indispensable tool to counter terrorism, based on the argument that who has nothing to hide has nothing to fear from whatever collection of information concerning them. Still, we should not forget that the "glass man" is a Nazi, totalitarian metaphor. Who wishes to retain a private, confidential sphere is automatically labelled as a "bad citizen" and can be the target of oppression.

Thus, the starting point for looking at data protection in a new perspective can be said to consist in highlighting the mechanisms required to counter the coming of the digital tsunami. However, in the age of networked persons, the Internet of Things, and autonomic computing, this means to be also afforded a general "freedom to disconnect", to have the right "to make silent the chip", as already remarked in connection with the

[27] M.Hildebrabdt-S. Gutwirth, „General Introduction and Overview", in M. Hildebrandt-S. Gutwirth, *supra* note 17, p. 4.

[28] S. Simitis, "Datenschtz — eine notwendige Utopie", in Summa. Dieter Simon zum 70. Gebtir stae. Klostermann, Frankfurt a. M. 2005, 511-527.

purchase of goods containing a chip that can allow information on the purchaser to be subsequently acquired.

The conditions applying to the electronic body and digital identity are similar, at least in part, to those applying to the physical body, given that the insertion of electronic devices into the human body or its dependence by the way some things are working can hamper one's autonomy to a greater or lesser extent and make one dependent on the outer world. A precondition for the insertion of a chip to be lawful consists first and foremost in the reversibility of the implant — which ensures that the individual can retain governance over their own body.

It is exactly in looking at the physical dimension of the individual that one cannot help raising questions concerning identity. "Is a hybrid bionic system a person, an entity one can attribute rights and duties on that account? (...) 1s the human user/component of a hybrid bionic system the same person before and after being so interfaced with artificial devices?"[29]

Identity is therefore shifting from a synchronic to a diachronic dimension, which also holds true if the individual is digitized and becomes part of an electronic network. It is the time-honoured topos of Theseus' ship, which can be conjured up nowadays as a token that can help us better realize how necessary it is to replace a static concept of identity by a dynamic one — whereby identity becomes as varying as the individual it applies to whilst its epistemological nature is unrelentingly reshaped. Subject is no longer compact, unified, neatly defined entity. It is enigma[30] rather than problem. It is becoming nomadic[31] - which mirrors the fragmented, mobile reality. It is no harbour — rather, it is process. And identity may be equated to the many "windows" that open on a screen. "These windows have become a powerful metaphor to conceive of the self as a multiple, distributed system"[32]. However, this multiplication of identities does not only result from the activities of several entities looking at the same individual from multifarious viewpoints. In cyberspace, the data subject can continuously take on different identities in order to better communicate and get rid of constraints that would hamper the free development of their personality. A

[29] F. Lucivero-G. Tamburrini, "Ethical monitoring of brain-machine interfaces. A note on personal identity and autonomy", in "Artificial Intelligence & Society", 2008, p. 451.

[30] C. Castoriadis, "L'état du sujet aujourd'hui", in Le monde morcelé. Les Carrefours du Labirinthe. III, Seuil, Paris, 1990, pp. 189-225.

[31] R. Braidotti, Nomadic Subject : Embodiment and Sexual Difference in Contemootarv Feminist Theorv, Columbia University Press, New York, 1994.

[32] S. Turkle, Life on the Screen. Identiy in the Age of the Internet, Simon & Schuster, New York 1995, p. 14.

necessary assumption in this scenario is the right to anonymity: even if it has been harshly questioned in the age of the endless war on terror, however it still remains a key component of citizenship in the new millennium. Indeed, there is no conflict between the permanent vindication of this right, which entails opaqueness, and the rampant social networking that is the utmost manifestation of transparency. There are increased options available to build up identity, and people must be in a position to make use of all those options.

We are faced ultimately with the concept of identity as a process, and this is clearly shown by digital identity management systems: these systems should arguably meet three core privacy requirements. The system must: (1) make data flows explicit and subject to data owners' control; (2) support data minimization by disclosing no more data is needed in a given context; and (3) impose limits on linkability"[33]. Still, these requirements, which are compounded of legal norms and privacy by design, should not be regarded as the ultimate solution — rather, they are markers to be used in order to enhance societal awareness of identity-related issues.

[33] P. M. Schwartz and a1., *supra* note 17, p. 278.