European Commission

JRC SCIENTIFIC AND POLICY REPORTS

The constitution of the hybrid world

How ICT's are transforming our received notions of humanness

Paula Curvelo
Ângela Guimarães Pereira
Philip Boucher
Melina Breitegger
Alessia Ghezzi
Caroline Rizza
Mariachiara Tallacchini
Lucia Vesnic-Alujevic

Joint Research Centre

Report EUR 26455 EN

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Ângela Guimarães Pereira
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 361, 21027 Ispra (VA), Italy
E-mail: angela.pereira@jrc.ec.europa.eu
Tel.: +39 0332 78 5340

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC87274

EUR 26455 EN

ISBN 978-92-79-35149-5 (pdf)
ISBN 978-92-79-35150-1 (print)

ISSN 1831-9424 (online)
ISSN 1018-5593 (print)

doi:10.2788/58678

Luxembourg: Publications Office of the European Union, 2014

Printed in Italy

The constitution of the hybrid world

How ICT's are transforming our received notions of humanness

Contents

PREAMBLE

The development and widespread use of information and communication technologies (ICT) are having a profound impact in many aspects of our daily lives, transforming the conditions and procedures of work, changing the modes of communication and social interaction, and altering the fundamental nature of human action, insofar as they play an important role in shaping what we do and how we experienced the world.

In fact, the re-conceptualisation of the very foundational assumptions of modern societies, the new configurations of natural and social life, and the blurring of ontological categories upon which our political, social and legal orders are based, point to fundamental aspects of the human condition that have been reshaped by the hybridisation processes characterising modern human entanglements with emerging technologies.

Despite the constitutional nature of these transformations, the basic rules that bind a state to its citizens have undergone small adjustments and accommodations. This not only shows how constitutional rights continue to be regarded as the most stable elements of national life, but also calls attention to the need of looking for the ways in which unwritten and emergent rules of constitutional dimension are being crafted.

Where can we observe the new constitutional order that is emerging at the present moment? What fundamental aspects of human life are being transformed by the mediated role played by new ICT? What are the far-reaching ethical, legal and social implications of these transformations? In what way the most fundamental human rights and the most fundamental relations between states and citizens are being reframed in view of cross-cutting transformations in law and new ICT?

In this essay we propose to address these questions by focusing our analysis on complex forms of mediation and translation that emerge from the use of the Internet and other ICT-based network arrangements. Hence, six technological settings: digitalisation of our bodies; governance of memory; internet of everything; drone age and surveillance; growing up, relating and connecting through social networks; and emerging spaces of political action, are the basis to address the complex interactions between the technology and its users and explore how they are now challenging what we received as fundamental Constitutional features.

1. SETTING THE SCENE

In 1998, in referring to the policies outlined in the U.S Department of Commerce's Statement of Policy on the privatisation of the Internet Domain Name System *(DNS)*, known as the "DNS White Paper" (NTIA, 1998), and the formation of the Internet Corporation for Assigned Names and Numbers (ICANN), David Post suggested that cyberspace was undergoing its first "constitutional moment" (Post, 1998). According to Post, the creation of a global governing entity with ultimate power to define the contours of cyberspatial existence worldwide was an exercise in a kind of constitution-making. However, as Lawrence Lessig noted at that time, “we are creating the most significant jurisdiction since the Louisiana purchase, and we are building it outside the review of the Constitution” (Krochmal, 1998).

In this paper we suggest that to better understand the full meaning of our current "cyberspace's constitutional moment" we must move beyond the high politics of Internet governance and focus our attention on the new kind of social contract emerging from the use of the Internet and other ICT-based network arrangements (Mueller, 2002). As Lessing argued, the "constitution" is not just a legal text, but a “way of life” - an architecture “that structures and constrains social and legal power, to the end of protecting fundamental values” (Lessig, 2006). It relates with the expanded sense of constitutionalism proposed by Jasanoff (2003), one that "will take on board the full range of processes by which individuals in modern society order their relationships with the institutions that govern their lives".

In fact, in our globalisation and hybridisation era, where the blurred boundaries between the cyberspace and the real space shake the referential frameworks on which policies are built (Broadbent et al., 2013), it is no longer necessary to hold a formal nation convention to rewrite the fundamental rights that bind a state to its citizens - "radical shifts in social order do not have to originate at, or even be confirmed by, the highest ranks of political authority" (Jasanoff, 2003). This new Constitution - which Latour spells with a capital C to distinguish it from the political ones - "defines humans and nonhumans, their properties and their relations, their abilities and their groupings" (Latour, 1993). In view of this wider meaning of "Constitution", we hope to better understand the mediating roles played by new ICT and to shed some light on how the complex interactions between these technologies and its users is providing the ‘material answer' to the moral question of how to act (Verbeek, 2005, 2006, 2011).

The inspiration for this endeavour was Sheila Jasanoff’s edited book, *Reframing Rights – Bioconstitutionalism in the Genetic Age*. In this book the term “bioconstitutionalism” is used to describe the major intersections between life-sciences, biotechnologies and the law in contemporary societies. The label not only captures the deep-going transformations in the relations between life and law, but also translates the way the different essays collected in this book interpret the far-reaching epistemic and normative implications of these cross-cutting transformations. By pointing toward fundamental realignments in the legal and ethical relations between human beings, their bodies, their relationships with other species, as well as their

institutions and norms of governance, the label "bioconstitutionalism" offers an interesting analytical framework to interrogate the current technoscientific revolution "that is at the same time also a revolution in humanity's capacity for self-understanding and self-control" (Jasanoff, 2011, p. 287).

As we hope to illustrate in the following sections, the application of this framework in the field of ICT opens up interpretative possibilities of the coproduction of epistemic, technical and social realities, and provides new insights into the tensions of the established legal and social orders. Indeed, even though there is increased recognition of the disruptive nature of new ICT, there is still a lack of understanding of how novel related entities, objects, techniques and practices are leading to a redefinition of the very notions of human identity, human dignity, citizenship, liberty, freedom, autonomy or property.

By exploring the rapid spread and pervasive nature of ICT in many aspects of life, we argue that the mutually constitutive interplay of digital and legal conceptions of human rights, duties and entitlements is a fundamental feature of the contemporary 'information/network society' (Castells, 2010; van Dijk, 2006). Accordingly, we suggest that to better understand the constitutional moment that characterises the hybrid world we are creating - *a world of new ontologies, blurring of private and public sphere, blurring in temporalities and spatial connections, strong metaphors of connectivity, social and political derangement, citizenship and consummership, etc.* - we need to critically examine the mediating role that ICT play in shaping the experiences and actions of those who use them and to take the normative and ethical implications of these mediating processes more seriously.

Hence, in the following section we propose to analyse the particular forms of mediation associated with six technological settings (digitalisation of our bodies; governance of memory; internet of everything; drone age and surveillance; growing up, relating and connecting through social networks; emerging spaces of political action) where the complex interactions between the technology and its users point to an increasing blurring of the boundaries that have been securing fundamental Constitutional guarantees: the distinction between nature, humans and artefacts, humans and non-humans (Latour, 1987, 1993, 1999) reality and *virtuality* (Castells, 2010; Hansen, 2006), and public and private (Habermas, 1991; Weintraub & Kumar, 1997) (see Figure 1).

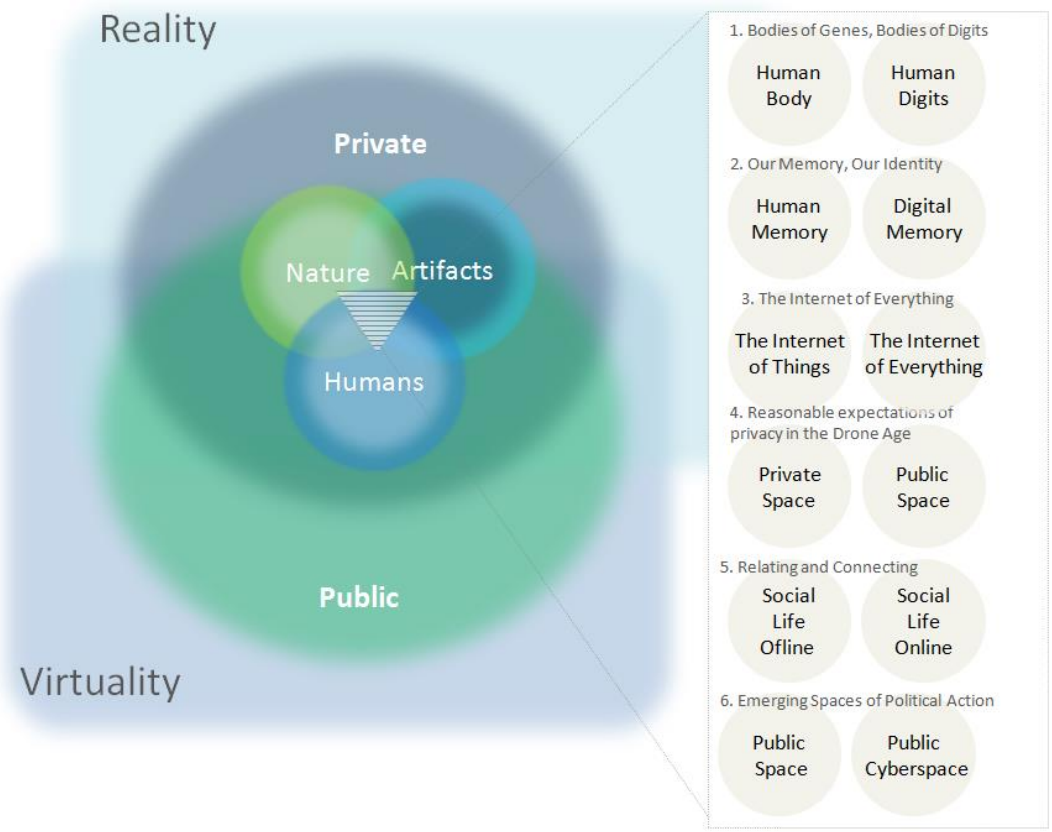

Figure 1. The Constitution of the Hybrid World

Hence, these six technological developments are begging the question philosopher H. Arendt asked on her book The Human Condition, *What are we doing?*

2. THE HYBRIDS

2.1. Bodies of genes, bodies of digits

The relations amongst life sciences, ICT, values and rights composing the uneven and shaded cognitive/normative landscape of contemporary democracies have been analyzed along several broad thematic lines. The human body sits today at the crossroad between divergent tendencies. On the one hand, the body has been widely de-materialized in order to make it readable, portable, mobile, and patentable (Boyle, 1996). Biological materials and their connected information have become the starting point for unprecedented forms of knowledge; the informational body is an instrument for health prediction; it is quantified in all its measurable and unmeasurable expressions; it can be self- and other-tracked and surveyed in its physical and psychological performances. On the other hand, the body is also increasingly relevant as the ultimate "material haven" to back-up and securitize the disembodied and rarefied digital self. For instance, blood samples from new born babies have been proposed as the ultimate validation for digital documents; [1] and the implantation of microchips is already taking place for individual and social forms of control. [2]

While some studies are concerned with potential future hybridized "post-human" machine-body cyborgs and other deterministic ways biotechnology is modifying what it means to be human; other approaches examine how biological, genetic and genomic research, genome databases, bioinformatics, combined with social networks, and crowd sourced knowledge communities. These analyses look at the contemporary convergence of the biological and informational, the movements back and forth between life and digits and how they tend to inform each other; namely how biological and information technologies are "more and more becoming a site of new engagements" (Castellanos, 2006).

The case for biobanks, namely the storage and use for research purposes of human biological materials and information, and their scientific and normative evolution, not only shows the complex interactions between the biological and the digital domain, and how they have mutually redefined each other, but also to what extent their having been deeply re-socialized through people networking saved their life. In fact, whilst biobanks were started as top-down, State-driven, public health-oriented initiatives, open exclusively to scientists and experts, they have mostly (and most successfully) evolved towards forms of genetic social networks, with direct citizens' involvement and engagement (with various degrees of real or rhetoric empowerment).

During the past thirty years human biological materials associated with personal, medical, and genetic information have become crucial for research, as well as for therapeutic uses, and their related commercial exploitations. In the normative puzzle that has taken place around their legal framing, the concepts of autonomy, privacy, and property have been played as defensive

[1] See, for instance, the initiatives listed on Infowars.com, http://www.infowars.com/articles/nwo/un_register_every_baby_born.htm

[2] EGE (European Group on Ethics in Science and New Technologies). 2005. Ethical Aspects of ICT Implants in the Human Body, Opinion N° 20, Adopted on 16/03/2005, available at http://ec.europa.eu/bepa/european-group-ethics/docs/avis20_en.pdf

tools to prevent and dismiss requests from the public to participate in decision concerning research and its potential benefits (Tallacchini, 2013)

Indeed, in the late 1990s some cases were turned down by citizens, who suddenly discovered that all their genealogical, medical and genetic information could be used with their presumed consent for the sake of human progress. Infamously, in 1998 the Icelandic Parliament, authorized by law the private company DeCODE Genetics [3] to build a National Health Database by collecting and storing all Icelanders' personal and genetic information through an opt-out system for consent. The initiative triggered a number of criticisms against the existence of an all-encompassing genetic social contract between the State and its citizens that escalated to courts (Winickoff, 2006).

After this experience, several technical and legal fixes have been used to tame citizens by convincing them that personal data and biomaterials were irrelevant once privacy was granted (through anonymization), and autonomy respected (through informed consent), reinforced by the moral prohibition against property rights on the body. Nonetheless, people remained quite skeptical towards top-down framed and managed biobanking, and reluctant to accept it. To some extent, biobanks' life has been "saved" by participatory mechanisms directly involving the public, especially after direct contact with potential participants was made easy through the web. Participatory and participants-driven initiatives in genomic research have been increasingly recognized as implementing the idea of scientific citizenship (Saha & Hurlbut, 2011), respecting individuals' dignity (Skloot, 2010), and reconciling individual and public health (Gottweis & Lauss, 2010; Tallacchini, 2013).

Genetic social networks and online collection of self-reported data are radically modifying the quantitative impact, timing, and working methods of research, and are also controversial from the scientific perspective. As it has been highlighted, "(r)esearch relying on collection of self-reported data by self-selected participants has known methodological limitations, including selection bias, information bias, and confounding" (Janssens & Kraft, 2012, p. 2).

Moreover, some normative concerns exist. Though reflecting a deep anthropological and social change towards bottom-up processes of collaboration and cooperation (Benkler, 2011), the shift towards "occupying science"(Saha & Hurlbut, 2012) is fraught with ambiguities, especially as to the rethinking of privacy. On the one hand, individuals are increasingly willing to set aside some of their concerns about privacy when their biological samples and personal information become part of a peer-production of knowledge of both scientists and citizens; and when participants can control and make decision about research and its benefits. On the other hand, the proposed substitution of privacy – depicted as a hypocritical promise—with the value of scientists' "veracity" towards participants (that their privacy cannot be granted anymore), combined with the presumed citizens' duty to "give back" to society for the benefits made possible by research, appears as a blunt legitimization for any use of data by the scientific community (Lunshof, Chadwick, Vorhaus, & Church, 2008).

[3] http://www.decode.com/

For the time being, genetic social networks have been mostly driven by the private sector. In reframing genetic investigations as "genomic personal services" sold on the web, companies such as 23andMe and PatientsLikeMe [4] have successfully advertised Direct-to-Consumer tests and genetic networking as forms of personal empowerment – besides their representing recreational, and not medical, activities (Koch, 2012; Saha & Hurlbut, 2011). The potential for sharing participants' data with third parties as well as the commercial uses of research findings remains not entirely disclosed or is justified as a constraint due to market mechanisms to make research benefits fully available to the public.

2.2. Our Memory, our Identity

> *"I want to introduce the "right to be forgotten". Social network sites are a great way to stay in touch with friends and share information. But if people no longer want to use a service, they should have no problem wiping out their profiles. The right to be forgotten is particularly relevant to personal data that is no longer needed for the purposes for which it was collected. This right should also apply when a storage period, which the user agreed to, has expired".* Viviane Reding address[5] at The European Data Protection and Privacy Conference in 2010.

But why do we need a "right to be forgotten" in a (hybrid) world that seems to celebrate memory and condemn forgetfulness?

Forgetting and remembering are both functions of memory; memory configures our identity. We can say that up until the connection and sharing hype that ICT are stimulating, our memory was somehow materialised, expressed and contained by the boundaries of our bodies and objects, being therefore somehow manageable. The issue of forgetfulness (expressed as erasure of data) appears now to be an emergent urgent issue especially because by design many of the technologies from which we are requiring forgetfulness were not designed to be forgetful.

Our memory is no longer solely installed in our bodies, on physical objects, diaries and logs or in our remembrance or in the songlines of the Aboriginal Australians[6]. Current "digital memory" technologies extend our memories in the form of bytes stored in our personal devices' chips or in the cloud. Our memory is a hybrid resulting from the variety of containers that we choose voluntarily or involuntarily to "store" experience and knowledge in a broad sense.

By the late 1990's, the transformation of the Internet was seen as going from "a medium or an information retrieval tool" to "a powerful archiving technology" (Lassica, 1998). In a very close future, when millions of devices will be connected through what is called the Internet of Things (see next section) the amounts of data generated and exchanged about a person will be humongous, further diminishing the agency of individuals to autonomously control their data destinies.

---

[4] 23andMe, available at https://www.23andme.com/; PatientsLikeMe, available at http://www.patientslikeme.com/help/faq/OurVision

[5] Available at: http://europa.eu/rapid/press-release_SPEECH-10-700_en.htm

[6] See Bruce Chatwin's Songlines published in the 1980s, Penguin Books.

The importance of "oblivion" or forgetting has been looked at from different perspectives including ontological, epistemological and pragmatic ones. Forgetting is an important part of memory; it is a normal function for humans in contrast with what is expected from computers: when our data are lost, this is considered a failure (O'Hara *et al.*, *op. cit.*). Blanchette and Johnson (2002)[7] underlined the importance of oblivion in the development of new technologies and in the management of personal or sensitive data, since "the control over personal information is not only affected through selective access, but also through selective retention of such information" (Blanchette and Johnson, 2002: p.xx). Retention of data such as from bankruptcy, juvenile criminal records, and credit history could mean that individuals have not a right to oblivion (institutional forgetfulness) and social forgetfulness. Indeed, the authors point out that new technologies are affecting social forgetfulness: "while critics of the panoptic society have justly remarked on the *ubiquity* of data collection practices, we underline how such practices invisibly extend the persistence of social memory and diminish social forgetfulness" (*Op. cit.:* 39).

Forgetting in general, is seen by many as a strength, as a positive filter in order to live better (Nietzche, 1873)[8], and in this hybrid world, as an emancipatory process, as giving the possibility to avoid malicious effects arising from the absence of this function (Dodge and Kitchin, *op. cit*.), a feature and not a bug that avoids stultification in thinking, where one is afraid to act due to the weight of the past (Bannon, 2006), and also a way to avoid information overload that poses challenges to retrieving and selectively deleting data (O'Hara *et al.*, 2006[9]); hence computers should be thought to forget (Bannon, *op. cit.:* 9-11). In fact, many authors suggest that forgetting should be an integral by design function of the process of designing and implementing digital systems that record and store personal data (O' Hara *et al.,* 2006: 361; Dodge and Kitchin, 2005). For example, Dodge and Kitchin (*op. cit.*) suggest that digital memory could mirror some of the characteristics of forgetting in human memory by ensuring a sufficient degree of imperfection, loss and error (Schacter, 2001) in order to overcome exploitation and pernicious data usage that could even incur in abuse of civil liberties.

We concur that the practical implementation of "forgetting" can be tricky from a technological point of view, unless this function was implemented in the technology by design; the fact is that these technologies that we want to demand to be forgetful were by design built to not forget responding indeed to exactly opposite political and business demands. Also, our digital memory is not only what we decide to post (our "digital footprint") or what others decide to post about us[10]; often what is at stake is not only what that information does to us but also what it does to others (Ettighoffer, 2008).

But this is not only about technology being dysfunctional. In his book, *Delete,* Mayer-Schönberger (2009)[11] sets the case to hold ourselves responsible for the ways in which our digital memories are governed in the web: "the truth is *we* are causing the demise of forgetting,

[7] Blanchette J.-F., Johnson D.G., (2002) .Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness . *The Information Society,* 18, pp.33–45.
[8] Nietzche F., (1873) *On the use and abuse of History for life.*
[9] O'Hara K., [all authors] (2006) Memories for life: a review of the science and technology *J. R. Soc. Interface* 3, pp.351–365
[10] See Koop, 2011 for the data shadow concept.
[11] Mayer-Schönberger, V, (2009) : The Virtue of Forgetting in the Digital Age, Princeton University Press.

and it is up to *us* to reverse that change*"* (*Op. cit.*: 14). Responsible usage concerns all, and to a greater extent the young "digital natives" (Prensky, 2001), which should become more knowledgeable about the dangers of making their lives available through the Internet with often consequent self-inflicting pains. We would argue that we have not made space for a wider societal debate to have a discussion of what social norms, *etiquette* and values should be subjacent to our presence in the virtual world and especially at the intersection of both the online and offline. Therefore, the ways in which we choose to publish about others and ourselves is often ignoring what we would reasonably adopt as social norms in the offline world; for many reasons, for example, indiscretion and effrontery are made easy (see, e.g. Bertolloti and Magnani, *forthcoming*).

We would argue that because forgetting is recognized as an essential function for memory governance, technologies denying part of our memory function raise an ethical issue. "Digital memory" technologies, in particular those that collect, store and transform our memory in form of digital data by consented or unconsented processes, are extending, reframing, normalising and transforming what should constitute memory of individuals and about individuals and their networks.

A "right to be forgotten" (RtbF) seems to be a response to the digital pervasiveness of our lives with all what it entails to the extent that one can talk about a hybridisation of our offline and online existences. The hybrid entity in which our biological and digital lives are becoming is resulting in the co-production and reframing of rights and duties that would not emerge were our digital, online life be insignificant. However, this right does not emerge without causing a number of dilemmas; in here we discuss only few that relate to the establishment of collective memory and identity.

1st dilemma: individual memory, collective memory

Philosopher Hannah Arendt (1953) recognised the dynamics between what constitutes the private and what constitutes the public; the public concerns what is seen and perceived by everybody, as well as the what is "common", what "assembles all of us together" which remains always connected to the individuals and their multiple perspectives. The public, she argues, has its foundations in the individualities, and the formation of the common relies on the expression of those; on the other hand the private is also constituted on the basis of what is public; "the private lies at the basis of the absence of the others; the private person does not show itself to the others, and that is why, it is as if it did not exist" (Arendt, 1958). So, this permanent interaction makes one sphere indissociable from the other. Never the public and private spheres have been so blurred as in our current times, with implications for the interdependency and co-creation of what constitutes private and what constitutes public; of what constitutes "private memory" and "public memory"; hence, of what constitutes individual identity and, collective identity and imaginary communities (Anderson, 1983). So, deleting, with the danger of de-contextualising existing information or simply creating knowledge gaps in the digital realm can impair the constitution of memory and identity.

2nd dilemma: 'Memory governance' — Which knowledge and what values may legitimately prevail?

Deleting in the digital world implies that a decision needs to be taken, especially on what constitutes 'public information', and for what concerns the RtbF, personal information that is of interest to public spheres. Hence, who's responsibility for deleting? Who determines what 'pasts' are told to upcoming generations? At least, this begs the question of what collective or historical right to be forgotten there is against the institutional media's perpetuation of a 'mainstream past' and who is veiling about it. Moreover, a 'right to be forgotten' could disregard the future value of information, i.e. deleted information could become valuable in the future — e.g. for biographical, historical or legal reasons. In a post-scarcity culture such as ours, where there is an abundance of data and processing, the new information infrastructure transcends time. It is unpredictable. What people want and need to forget changes over time and cannot be established *a priori.*

3rd dilemma: Forgetting and forgiving

The Internet often "remembers what people wanted to have forgotten" (Mayer-Schönberger, *Op. cit.*: 1). Thanks to its "eternity effect" (Waltz, 1997)[12], the Internet preserves bad memories, past errors, writings, photos or videos which we would like to deny later (De Terwagne, 2013). Bannon (2006) underlines the potential relevance of judicious forgetting (from justice to amnesty) in the context of new technologies. In judicial cases, a RtbF could amount to a right to be forgiven and eventually the danger of denial. O'Hara *et al.* (2006) argues that forgiving may strike a "better balance between avoiding present-day conflict while respecting those who have suffered in the past". This may lead to moral discussions, especially with regards to public cases, and the construction of collective memory.

2.3 The Internet of Everything[13]

Our third case is about the ubiquitous, pervasive and transformative power arising from the digitalisation in which many of us live (in or with) today. The case is about ubiquitous connectivity of *everything*: people's things through things (natural, manufactured, material and virtual) and through their own bodies (e.g. through wearable or implantable "things"), the data these interactions generate and their processing. "Everything" also means that interconnectivity permeates spheres of life that are described as our humanness like our body (health), how we eat (food), our intimacy (relationships), how we spend our time (lifestyle), what we learn (knowledge), etc. For many of these "spheres" there is a tradition on ethics embedded in rights and norms that we have been living with. The issue then is how connectivity, that in the case of IoE creates new ontologies, entities and identities, hybridizes objects and subjects, entices or creates different relationships and skills based on fast (often) concealed interactions is challenging the existing normativity.

The expression we use here slightly extends what became known as the Internet of Things (IoT), i.e. a smart environment that will "enable computing to melt invisibly into the fabric of our

[13] This expression first appeared in CISCO, a consulting company. http://www.cisco.com.

business, personal and social environments, supporting our economic, health, community and private lives" (EC 2006). In the IoT scenario, “everything” becomes smart: smart energy, smart health, smart buildings, smart transport, smart living, smart cities (Vermesan *et al.* 2011). Both “physical and virtual ‘things’ have identities, physical attributes and virtual personalities, use intelligent interfaces and are seamlessly integrated into the information network” (Vermesan *et al. op. cit.*). Physical “things” (inclusive of humans) have digital counterparts and virtual representations. In this cosmology, *we* - meaning human beings with our bodies - relate to our environment just like any other entity, through our multiple digital counterparts and virtual representations.

The IoE is defined by strong mediation, through both embodiment and hermeneutic relations between humans and artefacts (Verbeek, 2006). In the former the “artefacts” are incorporated by users, becoming extensions of the human body or mind enhancing the interface between humans and the environment (e.g. glasses, implantable devices); in this type of relations the artefacts are not perceived. Hermeneutic relations on the other hand refer to relations where the artefacts provide a representation of reality requiring interpretation, decisions being taken based on such interpretation (e.g. a thermometer, wearable sensor). With IoE both types of relationships are emphasised and hybridised; users are likely to stop “noticing” the artefacts (sensors, RFID tags, cameras, etc.) that communicate among themselves in *autonomous* ways, and at the same time through the algorithms and models driving their activity these artefacts encapsulate representations of reality and worldviews. This latter condition, amounts to a deeper form of not “noticing” technology; it is not only about the artefact but also, more importantly, about the invisibility of the interaction itself (data transfers, decisions and action). Voluntarily or not, the user will need to rely on models and technology to achieve the chores that technology is meant to help her/him with (Stahl, 2011). Hence, the strong mediation inherent to IoE developments, will lead eventually to shifting or delegation of human autonomy and agency to the objects of the IoE. If noticed, artefacts will act on the user’s behalf; if not noticed, artefacts will act on their developers’ worldviews, intentionality and interests. This strong mediation poses challenges to human agency.

IoE could easily end up reinforcing the divide between capable users and those intimidated or outpaced by new technology. We refer here to diffuse divides that the unauthorised and unquestioned automations, seamless transfers and unnoticed ubiquity of IoE may create. With IoE, where the promised interconnectivity involve billions of both smart human and non-human “objects” and transactions for which mechanisms of authentication and consent need to be put in practice, consent may become an absurd concept. Those who are knowledgeable and skilled enough and empowered to control the working of the technology will master it, will be able to protect themselves against abuse, and to choose amidst the technological offer or opt-out would they deem it necessary. The divides in this case are not exclusively related to lack of skill to deal with the complexity of interactions, but also to what we could call “consent fatigue”, which poses additional challenges to all individuals and most notably to those with reduced autonomy, such as children and the elderly. Hence, the rising divides in these cases have, paradoxically, implications for knowledge production, skills development and empowerment. Those who cannot keep the pace with the pervasiveness will progressively become deskilled, disempowered and unknowledgeable, their agency being compromised.

Profiling became the nightmare of social and legal scholars with many recent ICT developments (see Hildebrandt and Gutwirth, 2007). High level of connectivity, seamless transfers and embedded intelligence of objects and machines cannot but make one think of scenarios where human autonomy and agency about even mundane decisions and activity is put in jeopardy. As an algorithmic procedure over data, profiling follows the logic of identification, categorisation and clustering of those who developed the algorithms used for such purpose. But such algorithms are blind to specificities of individuals. They act with indifference with respect to context in which the data they use were collected resulting on "things" collecting and storing our data, forming a multiplicity of 'dossiers' on our whereabouts that may be used in unexpected contexts (De Hert, 2005; Hildebrandt and Gutwirth, 2007)[14][15]. With the IoT promised levels of data transactions and embedded intelligence, profiling will lead yet to another level of disempowerment: the crucial issue is not abuse, but the fact that users will have no effective means to know whether and when profiles are used or abused (Hildebrandt and Gutwirth, op. cit.).

In the ubiquitous world of IoE there won't be the Orwell's "big brother" to blame or to refer to; a myriad of human and artificial agents are implied in the interconnected smart artefacts and machines promised in the IoE world view. Such developments will lead to a "*Some brother controls, knows and never forgets society*"(Mannesmaa, *2007*)[16]. "Some brother" is not a single agent, but a heterogeneous "mass" consisting of innumerable social actors, e.g. public sector authorities, citizens' movements and NGOs, economic players, big corporations, SMEs and citizens. The diffuse nature of the interactions, which inevitably results in changes of a user's agency with regards to artefact-to-artefact or machine-to-machine interactions, will result on opacity when it comes to decide on agents' responsibility, accountability and eventually agents' liability.

Considering objects' agency we look at the intentionality implied in objects' activity and what we can call a "contract" between objects and people and the hybrids that result from these interactions, namely subjectification and objectification (see Foucault). Embedded intelligence, seamless transfers and unpredictability[17] of the things in the IoE pose serious challenges to human agency. To which extent is there in the interconnected world of IoE conceptual equality between human, non-human and hybrid "objects" with respect to intentionality? Are people and objects just connected physically and causally, or also intentionally or symbolically? Can we attribute dignity or responsibility to non-human objects?

Numerous current examples of ICT developments include devices that take autonomous decisions (e.g. in healthcare or search and rescue situations (Stahl, *op. cit.*), the moral qualities of which are pre-established in algorithmic ways. Many automated technologies make it unnecessary and often undesirable for human users to exercise control over their own

[14] De Hert, P. **A right to identity to face the Internet of Things,** p. 5 at http://portal.unesco.org/ci/fr/files/25857/12021328273de_Hert-Paul.pdf/de%2BHert-Paul.pdf

[15] M. Hildebrandt and S. Gutwirth (EDS), 2007. Profiling the European Citizen. Cross-disciplinary perspectives.

[16] Mannermaa, M. 2007. Living in the European Ubiquitous Society. Journal of Future Studies 11(4):105-120

[17] Objects and services potentially accessible from anywhere at any time, may result in unpredictable emergent behaviours – see for instance, Wright *et al., op. cit.* in their discussion of ambient intelligence's key characteristics.

behaviour; this is what has been termed the *self-miscontrol* trap (Crabb, 2010)[18], i.e. a failure of people self-control when their behaviour is controlled by pre-designed social and moral norms in technological devices. People are often compelled to use technology as something inevitable otherwise risk being isolated; up until recently we could argue that it is the users' appropriation of technology that dictates major categories of intentionality, responsibility and accountability. With the promised automation in IoE, this attribution can be at least questioned; in a IoE world vision, intentionality is at most shared among creators, designers and users of technology; all human agents need to be identified for their intentionality, the morals they sustain, otherwise the risk is that no responsibility can be attributed once the objects mediate and operate within a IoE.

Hence, with this scenario we may want to ask ourselves about what humanness features are being transformed with and by technology.

2.4. Reasonable Expectations of Privacy in the Drone Age

Unmanned or remotely piloted aviation systems (UAS/RPAS, colloquially 'drones') are most often associated with counter-terrorist surveillance and combat operations. Recently, however, their significant potential in non-military applications has been recognised in Europe and the USA. Amongst the hundreds of anticipated applications, the most lauded would reduce risk to human life, e.g. firefighting and search and rescue. Others would improve the efficiency and effectiveness of existing commercial services such as mail delivery and aerial photography. Some applications may be more controversial, e.g. enhanced police surveillance and search of citizens. Interest the gamut of these applications has culminated in European and US strategies for the integration of non-military drones in domestic airspace, allowing them to be fly alongside manned aircraft. Here, we consider how this process of integrating drones into regular airspace could affect the relationships between technology, society and the law, with particular reference to the legal and personal experience of privacy.

Since the 2009 Modernization and Reform Act (P.L. 112-95), the Federal Aviation Administration (FAA) has been responsible for overseeing the integration of drones into the regular US airspace from 2015. Similarly, the European Commission (EC) set up the European RPAS Steering Group (ERSG) in 2012 to establish a roadmap (ERSG, 2013) for the integration of drones in European airspace from 2016. Both explicitly recognised that privacy may be compromised by drones' surveillance capabilities and the US programme was delayed to consider the issues more carefully (GAO, 2013; Huerta, 2012)[19].

It is often said that the personal experience of privacy in the US is about liberty and protection from the state, whereas in Europe it is about dignity and protection from personal intrusion (Newell, 2011). This difference is reflected in legal terms. US privacy laws primarily protect citizens from state search and seizure, whereas European privacy laws primarily protect personal dignity (Whitman, 2004). Here, we first consider drones in the context of state

[18] In Crabb, P. B, 2010. Technology traps: who is responsible? Technoethics. 1(2).

19 For a summary of common concerns, see the petition by the Electronic Privacy Information Center (EPIC, 2012).

intrusions of privacy, primarily in the USA, before considering how drone development might intrude upon the personal experience privacy, as emphasised in Europe.

State Intrusions of Legal Privacy: In the USA, citizens' privacy is protected from state searches under the Fourth Amendment. The state must obtain a warrant by demonstrating probable cause of criminality before the search. This approach to legal protection of privacy reflects the cultural understanding of privacy as freedom from state intrusion. Indeed, in the debate about drones, the arguments of supporters and opponents of drone development are both frequently aligned with this anti-interventionist position. [20] Here, we consider how the proliferation and normalisation of drones in domestic airspace can affect the legal domain of privacy from the state.

The boundaries of what constitutes a search (requiring a warrant) are defined with reference to a reasonable expectation of privacy (REP). This depends upon two conditions. First, a 'subjective' condition that the expectation of privacy is actually held by the individual and, second, an 'objective' condition that this expectation is considered reasonable (e.g. by a jury in a criminal court). In *Katz vs. United States*, the Supreme Court upheld the defendant's right to privacy when he used a public telephone for illegal gambling. As such, the wiretap deployed without warrant constituted an illegal intrusion of privacy and the evidence collected through it could not be submitted. This example shows how the proliferation and normalisation of an ICT artefact (telephone booths) can enable privacy in places as busy as the streets of New York City. In a pertinent counterexample, however, we can see how other technologies have diminished the domain of privacy from state intrusion. At the time the Fourth Amendment was introduced, a warrant was required to search beyond solid fences surrounding private property. Since then, police have conducted searches from helicopters and aeroplanes without a warrant. Objections based upon REP are rejected because the proliferation and normalisation of the technology meant that it was unreasonable to expect privacy from aeroplanes under normal airspace (Thompson, 2013).

The example demonstrates how technology development can affect the legally protected domain of privacy and the consequences for drones should be clear. By 2015, drones may also be deployed in normal navigable airspace and their rapid proliferation and normalisation is expected soon after. While deploying many of the same technologies such as motors and cameras, their character and scale could present qualitative differences to manned aircraft; sufficiently small and quiet to go unnoticed, sufficiently cheap and independent to run persistently, sufficiently modifiable to capture visual, heat, odour and sound profiles. McGill and Kerr note that "whether privacy-intensive or not, once an investigatory technique is standard practice, it soon becomes unreasonable for people to expect the police to act in any other way" (2012, p. 210). Can anyone who read about the Snowden revelations in the summer of 2013 expect total privacy in their online activities? Likewise, following a proliferation and normalisation of drones, could anyone reasonably expect shelter from the advanced state

20 Opponents have argued that drones should not be allowed to develop, as they will be used by the state for excessive surveillance of citizens. Meanwhile, supporters have argued that the state should not intervene in technology development by restricting domestic drones. Indeed, some want personal drones equipped with weapons to exercise their right to bear arms (FAA, 2013).

surveillance capabilities? By facilitating the integration of UAS into domestic airspace, do the FAA risk abbreviating the domain in which citizens' privacy is protected by their constitution?

Intrusions of the Personal State of Privacy: Of course, privacy is more than a legal right; it is a personal experience that citizens value. It is as subjective, malleable and unpredictable as any other personal experience. The diminished expectations of privacy resulting from technology development, as considered above, may provide a useful starting point. Regardless of its legal impact, if we do not expect or believe that a state of privacy exists, can we truly experience it? What happens to society when a commonly valued experience such as privacy is erased or reduced to doublethink? We cannot answer these questions here, but can consider how drone development may have a diminishing effect upon the personal experience of privacy.

Despite knowing that a fenced garden can be occasionally seen, the place can still foster the personal experience of privacy. The regularly passing air traffic (cargo and passenger planes) is not for the purpose of surveillance, and those that are (such as police helicopters) are rare and announce their presence loudly. Drones are different. Their subtlety, economy and enhanced capabilities differentiates them from police helicopters and satellites. As Google's Streetview cars gleaned data broadcast from poorly secured WIFI networks, drones could collect and analyse heat profiles 'broadcast' from people's homes to sell information on household practices. The drones may be operated – lawfully or otherwise – by police, private companies, individuals, spies, criminals and terrorists. The identity of the operator and purpose of the flight may be obscured or spoofed. How can the citizen know who owns or operates a given drone, what surveillance equipment it carries, what data it collects, what purpose it is collected for, how long it will be kept for, who it can be sold to, and how they can respond? Assuming the level of development predicted by enthusiasts and critics alike, the proliferation and normalisation of drones could diminish the personal experience of privacy felt behind fenced gardens and inside homes.

Studying responses to privacy concerns a public hearing held by the FAA (2013), the counterclaims fall into three categories. The first rejects privacy concerns as public misunderstanding of technology. The second accepts the possibility of privacy concerns, but argues that only a specialist authority should handle such concerns, not technology and aviation specialists such as the FAA. Finally, the third accepts privacy concerns and the need for technology developers to address them to ensure that developments are aligned with citizens' values. However, the only practical solution offered in this regard was the requirement to make all drone operations public by broadcasting the owner, operator, flight purpose, data collection and subsequent use. This approach is aligned with 'open technology' and 'privacy by design' ideals and may be well intended but, as the citizens are increasingly informed of the surveillance they are subjected to, their reasonable expectations of privacy can only be decreased. This has implications for their legal right to as well as their personal experience of a state of privacy.

2.5. Relating and connecting

A social networking site (SNS) is a website where users can create a profile and connect to others in order to form a personal network (Lenhart & Madden, 2007). Social network (SN) consists of its users' representations (a "profile"), their social links ("friends") and additional services to facilitate the interactions between "friends", such as e-mail, postings of various media content (pictorial, film, audio, textual, etc.) and instant messaging (Capurro et al., 2011). SNS are more and more popular among young people and older ones. SNS and their usage have been transforming our way of communicating and interacting, as well as making the boundary between offline and online worlds highly porous (see e.g. Coll, Glassey, & Balleys, 2011; Kember & Zylinska, 2012; Stokes, 2012). These transformations do not come without social, ethical or legal challenges. One's personal identity construction and 'perceptions' about it by others is now a hybrid encompassing one's offline self and online self; ideas of relationship and friendship are being deeply altered experimenting with and reshaping existing social norms; the attempts that are being made to translate legal provisions and fundamental rights that regulate our offline life to the "cyber-space" are not a simple one-way process: emerging online norms and ethics need to be taken into consideration.

One's identities: for Vallor and Shannon (2012) SNS constitutes a new space where real and virtual personal identities are constructed, presented, negotiated, managed and performed. SNS is a *"technology of the self"*: on the one hand, it facilitates the construction and performance of personal identity in both real and virtual worlds; on the other hand, personal identity is built and performed through distinctive kinds of communal norms and moral practices generated by SNSs. Stroke (2012) argues that online SN offer more methods to users to manage their self-presentation than offline social spaces (i.e. home, school or work). He shows that these virtual identities are not the ones established in the offline world but the hoped-for possible identities, users wanted to have in the offline world but had not yet been able to establish. However, Parsell (2008) and Turkle (2011) highlight the risk of reducing people to their SNS profiles and their personae in the virtual world, constricting one's identity to a closed set of communal norms. This risk of being characterised and seen through the exaggeration of one singular trait leads to the '*deindividuation*' of SNS users' personal identity, who consequently are perceived as representatives of a group instead of unique persons (Parsell, 2008). The absence of face-to-face interactions reinforce this tendency and may contribute to the diminution of "passive mode of embodied self-presentation" (i.e. body language, facial expression and other spontaneous displays of emotion), which are a constitutive part of one's whole identity (e.g. Cocking, 2008; Vallor, 2012).
In many European countries the right to personal identity has been established in their legal systems under the rights of personality, reaffirming the right for a person of being individuated and identified i.e. the right to *"possess, control and impose a set of particular characteristics and features which individualized and distinguished her from all the others",* while the rights of personality have emerged from the need to safeguard the value of human dignity, to protect juridical interests and values deeply related to the human person (e.g. life, physical and moral integrity, honour, reputation and privacy) (Andrade, 2011, p. 70) – this right constitutes a human right both through the United Nations Convention on the Rights of the Child, Art. 5 and the European Convention on Human Rights, Art. 8.

Negotiating friendship in a hybrid world*:* virtual and real relationships are not in competition but they feed into each other perhaps breeding newer ontologies; *"virtuality"* tends to skew our experience of the real in several ways: *"denatured and artificial experiences seem real"*, the *"fake" becomes "more compelling than the real"*, and virtual experience may be so compelling that one could believe that within it they have achieved more than they have (Turkle, 1996).

This is particularly relevant when one looks at "friendship" concept on SNS. Facebook is *reworking what we understand as a "relationship" and a "connection"* (Kember & Zylinska, 2012, p. 158), and though offering many positive things (such as enhancing friendship, family connections, etc.), Turkle's (2011, p. 19) notes that through our new way of communicating and interacting via social media, or mobile devices *"we are increasingly connected to each other but oddly more alone: in intimacy, new solitudes"*.

The "*Friending process*" (Boyd, 2006) that SNS provides as a means to organize friendships, requires the creation of a profile where users are first asked to choose people and then their interests. She considers that users define their community *"egocentrically"*: their list of friends determines the context, defining the relevant audience for their posts or for modifying their profile. Hence, "*Combined with profile content, friends serve as a signal to all visitors about the relevant context"* (Idem). Moreover, boyd argues that when people articulate their relationships on SNS, they are not simply projecting their internal model of friendship; based on an internal understanding of the audience, they override the term "friend" to make room for a variety of different relationships so that they may properly *show face*. But what is the difference with the physical world? In fact, she underlines that the negotiation of friendship on SNS (accepting or rejecting) is deeply connected to users' offline social life: each choice can modify or complicate relationships with friends, colleagues, lovers, etc. SNS *"are not digital spaces disconnected from other social venues — it is a modeling of one aspect of participants' social worlds and that model is evaluated in other social contexts."* (Idem). Hence, not surprisingly phenomena like (offline) violence may find a correspondent space in the digital space.

The cyber-bullying phenomena[21]*:* SNSs can be better described as dwellings where people act out their lives. People spend a great deal of time in these dwellings, SNS becoming the place where they – teenagers in particular - co-develop their identities and start their biography. The idea of a hybrid space is again relevant here: users of social media stop noticing them at a certain point (Trottier, 2012). However, due to SN "undifferentiation" between levels of friendship, users cannot rely on sub-group defense mechanisms as they would in "real life" when confronted with harmful attacks to their reputation and hence, dignity (Bertolotti & Magnani, forthcoming). Leiter (2010) relates how by refusing to link a professor's blog from his own blog (i.e. what we consider as a kind of rejection of SNS's friendship) he became victim of

[21] Form of aggression (humiliation, harassment, social exclusion, mockery, unpleasant comment, etc.) through the use of at least one technological medium and involving intentional, harmful, repeated behaviour on the part of the perpetrator within the context of an on-going social interaction (e.g. David-Ferdon and Feldman, 2007; Kowalski and Limber, 2007; Alvarez, 2012; Ortega et al., 2012; Rizza and Guimarães-Pereira, 2013).

"cyber-cesspool"[22]. We consider his experience as an illustration of how a 'simple' action in the virtual world (e.g. rejecting a SNS friendship) has consequences for offline social life. Leiter underlines that in the United-states *"current law provides almost no effective remedies for tortious harms, and none at all for dignitary harms (…)"* (Idem, p. 155). He argues that the harm of speech in cyber-space is sufficiently serious to rethink the US legal protections afforded cyber speech causing dignitary harms. In the EU context, Rizza and Guimarães Pereira (2013) shed light on how cyber-bullying is about challenging the integrity, dignity, personality and reputation of the person, and consequently questioning the right to freedom of expression[23]. Considering that cyber-bullying is simultaneously the cause and outcome of damage to an individual's reputation, they make the distinction between the right to privacy and the right to identity i.e. the transmission of information to the public sphere, correctly and accurately expressed. Therefore, in order to frame a possible regulation of cyber-bullying and strategies to cope with it, the authors argue that protecting one's privacy cannot be the main focus of such strategies and that the application of an 'identity right' to published facts and information provides an added incentive to strike a better balance with the competing right to freedom of expression.

This hybrid is interrogating and transforming norms and the value of personal relationships as well as the redefinition of the self and identity (Haraway, 1991; Jasanoff, 2003; Andrade, 2011); in fact it is adding to the existing spaces where power dynamics are developed and tested leading to reconceptualization of personal relationships, of community formation and in extreme cases to phenomena such as cyber-bullying. These types of phenomena, often transposed from the offline world, compromise further our human dignity, namely putting additional threats to the construction of the self for one's identity and personality both online and off-line, therefore requiring that the intertwining between the online and off-line codes of conduct are reflected upon also in law (Shariff, 2008).
The attempts that have been made in the legal realm to cope with the changes that are occurring through this hybridisation are bound by insufficient knowledge about these processes: co-production of the online and offline, the private and the public, the individual and community, and the social and the legal.

2.6. Emerging spaces of political action

The neo-liberal globalization that appeared at the end of XXth century brought the diminishing role of nation-state sovereignty and along with it the challenges for the development of democracy, citizenship and public sphere on a supranational level. The new media became an integral and many times central part in citizens' everyday lives. Since citizens are increasingly using Internet to engage with political life, this is often seen as a valuable tool for deliberative democracy and the involvement of citizens (Dahlgren, 2004). It also offers a potential to revitalize political participation and communication between political actors and citizens

[22] *"an amalgamation of what I will call "tortious harms" (harms giving rise to causes of action for torts such as defamation and infliction of emotional distress) and "dignitary harms," harms to individuals that are real enough to those affected and recognized by ordinary standards of decency, though not generally actionable"* (Leiter, 2010, p. 155)
[23] Articles 1, 3, 4 and 11 of The Charter of Fundamental Rights of the European Union (European Union, 2000).

(Coleman & Blumler, 2009). However, new technologies cannot themselves produce the so called "democratic nirvana"(Lusoli, Ward, & Gibson, 2006). The expansion and advance of the Internet could sustain the deliberation and political talk beyond the one of official communicators (Gastil, 2000), which could contribute to the augmentation of political participation offline(Vesnic-Alujevic, 2011; Wojcieszak, Baek, & Carpini, 2010). Because of the interactive nature of new media, where citizens are co-producers, co-distributors and active participants in online debates, one can talk of a new kind of synergy between ICT development and democratic renewal (Flew & Young, 2005). This approach to online deliberation is close to the idea of a Habermasian public sphere, with the interactivity and participation in the domain of public engagement and potentials of the global reach of the Internet.

The traditional concept places citizenship, placed within the boundaries of a state with rights that are voted and enforced through the rule of law, is changing into a dynamic concept, "evolved from the struggle for equal political and social rights for all" (Cammaerts & Van Audenhove, 2005, p. 179). The normative concept lacked the difference between a civic actor and political consumer (Coleman, 2005) and it was transformed due to globalization and potentials for interactivity and participation, offered by the new ICT. It is often said that there is a crises of citizenship, caused by a general dissatisfaction with formal policies, but we can see that between Lippmann's (1922) "deaf spectator" and Coleman's (2005) "disconnected citizen" the differences are minor.

The Internet has grown over time into a political space, where there is a possibility for citizens to get involved in politics by questioning, commenting and influencing, and consequently changing the power balance (Coleman & Blumler, 2009). However, the quality of online deliberation and communication is still questionable, as well as ability of citizens and the public sphere to influence social and political institutions (Calhoun, 2002).

In the context of technologically mediated citizenship, it is arguable if the new technologies offer a new framework for citizenship or help only with the construction of "elite citizens", who are already included in community (Sujon, 2007).

Coleman and Blumler (2009) argue that the Internet has the potential to revitalize political communication, which brings them to the position of social constructivism, where meanings of ICTs are co-constructed by various actors and interests. Five democratizing characteristics of the Internet were suggested: active use (choice of a website, link etc.), discursive role (large number of users), inexpensive access to a great amount of data, and peer-to-peer and many-to-many interaction, which could bring up new ideas and approaches (Idem).

The links between citizenship and new technologies are broad and depending on how the interaction between the two is defined, it can include discussions centering around civil society, media literacies, social movements, communities, public spheres, local and transnational spheres, government and many others (Sujon, 2007, p. 204).

The Internet extends public space, which could serve as a transnational or global public sphere, a place for the exchange of ideas and challenging the opinion of others, as defined by Howard (2005) based on Habermas ideas. This hybrid online public sphere could fully develop through the Internet, because web 2.0 has facilitated citizens' online interaction and participation, and

this could lead to better inclusion of citizens in the public life and more deliberation (Vesnic-Alujevic, 2011) an optimistic sense of democratisation that does yet to overcome other types of political constraints. In fact, those constraints are transposed from the offline world, i.e. they did not get resolved with the advent of the Internet. For example, transparency of actual influence of the debates in political life, a low level of interactivity among citizens and a weak quality of debate are still major obstacles.

The Internet promotes certain societal values and rights such as equality or diversity, but the digital divide is still an issue with regard to building a more democratic society on a global level. There is still roughly 65% of world population without the access. In connection to that, there has been a debate about access as a potential human right. Frank La Rue, UN Special Rapporteur on the right to freedom of opinion and expression, in his 2011 report for instance, mentions that the right to freedom of expression implies the use of Internet and we should never be deprived of the Internet access. Besides, the Internet potential is seen as a foundation for many other rights. The availability of infrastructure (ICTs and software) and access to content without restrictions are highlighted in La Rue's report. Based on this report the UN declared Internet access as a human right. In some countries, such as Estonia, Spain, Finland, all citizens are entitled to access the Internet.

Access to the Internet gives humans access to human capabilities that "are considered fundamental to a life worth living" (Wicker & Santoso, 2013). Although some argue that the access to a technology itself cannot be a human right (Cerf, 2012), its access is fundamental to ensure the rights of individuals, such as the right to information, the right to free speech and freedom of expression (*idem*). Cerf (2012), recognized as one of "the fathers of the Internet", considers the Internet not as a single technology but as a sociotechnical network with different technical tools, customs and organizations.

The access to content is related to the censorship done by the state mostly, such as blocking and filtering the information (as in Egypt, for instance), criminalization of the freedom of expression as in China or disconnecting people from the Internet access as in certain cases in France.

The emergence of new spaces of political deliberation, development of democratic institutions at a supra-national level along with the diminishing role of the nation-state sovereignty and changes of power relationships between citizens and the institutions that govern their lives, such as the State and Corporations, points to a new constitutional order in this hybrid space of interactions. Citizens engage in online deliberation, interact with other social actors and participate in decision-making processes redefining the notion of citizenship itself. What emerging rights can be associated with these changes? What emerging duties can be associated with these changes?

3. Discussion

The nature of contemporary human action is inextricably bound up with new forms of technological mediation that shape the relations between humans and the world and transform both experience and action. Indeed, technological artifacts are more than functional instruments, they "coshape both the way human beings are present in their world and the world is present for human beings" (Verbeek, 2005, p. 172).

As the examples presented in the previous sections suggest, the new Constitution that is being drafted in the context of modern human entanglements with new ICT is reshaping the dynamics of social order at many levels. This new Constitutions is defining an all-encompassing genetic social contract between the State and its citizens; the ownership of human biological materials; the private property rights in one's own body; the working methods of medical research; the boundaries of what constitutes an illegal intrusion of privacy; the personal experiences of privacy, dignity, freedom and autonomy; the social norms of conduct; the basic ideas of personal relationships and friendship; the very notions of citizenship, nationhood and identity; the moderns imaginaries of democracy; and the new spaces and forms of political deliberation (Figure 2).

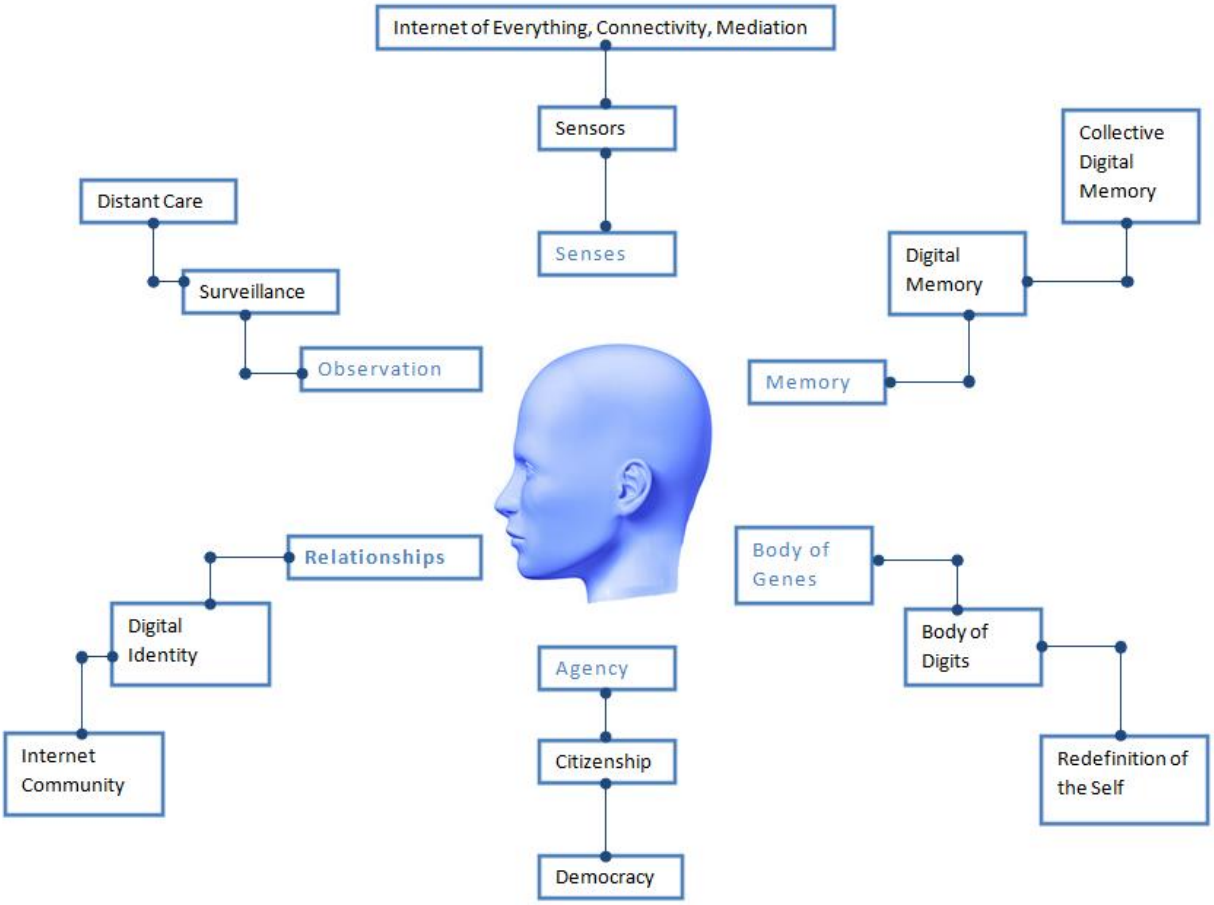

Figure 2. Basic features of humanness in the digital world.

And thought the legal issues are beyond the scope of this paper, thinking of reframing rights within situated constitutional contexts is still relevant here for several reasons.

First, different constitutional contexts not only derive from heterogeneous historical and cultural environments and express different ideas of citizenship; they also embody, convey, and further promote different visions and meanings of rights. For instance, the perception of health as a constitutional right, while deeply rooted in European citizens, has no parallel in the US. Conversely, the idea that owning weapons is an individual right – renewed by the US Supreme Court a few years ago—does not belong to European rights.

Second, when technoscience become an essential part of constitutional changes, it also enters a complex process of co-production with law and society, making rights even more characterized by specific technoscientific and legal cultures. In the ICT domain, for instance, the US and EU rights to privacy do not share the same meaning and content.

Third, that especially in the domain of technoscience where many "divides" – health, wealth, generational, educational, digital, etc. – separate people and countries, the discourse about rights should be mostly understood in terms of actual capacities and abilities (Sen…).

Fourth, in the specific context and contingency of the European Charter of Fundamental Rights of the European Union, whose entering into force (ad the end of 2009) has the potential to radically alter the original States-based ontology and way of functioning of European treaties towards a citizens-based and citizens-driven European Union, the reframing of rights through the deep co-productionist moves engendered by bio-and cyber technosciences can be also connected to a deep reframing of the Europe that citizens want.

For all these reasons – and many others, such as (just to mention a few) the supposedly universalizing characters of science and technologies; the presumed and real effect of globalization of markets and technologies; the globalized uneven texture of citizens and users of technoscience - the awareness that rights cannot be adequately defined and discussed in under-determined universal ways, but within specific cultures of rights needs to be maintained.

In fact, this explanatory power of thinking of natural and social order as being produced together leads the participatory ideals of public engagement, with all the reservations pointed out by Wynne (2007), far beyond narrow perspectives of problematising the relationship between science and democracy. In fact, a more sophisticated model of public engagement with science and technology has been suggested for some time, one that acknowledges that 'public engagement needs to move upstream' to consider new ways of listening to and valuing more diverse forms of public knowledge and social intelligence (Felt & Fochler, 2009; Wilsdon & Willis, 2004). The basic assumption underlying the notion of 'upstream public engagement' relates with the necessity of replacing the one-way normative model of public 'understanding' of (or 'deference' to) science (Wynne, 2007, p. 100) to a more substantive model of engagement, which aims at creating more socially-robust scientific and technological solutions by way of opening up questions, furthering debates, exposing differences and interrogating assumptions. The ultimate challenge is 'to generate new approaches to the governance of science that can learn from past mistakes, cope more readily with social complexity, and

harness the drivers of technological change for the common good' (Wilsdon & Willis, 2004, p. 24). What seems to be at stake is not only the need to clarify the assumptions and arguments that sustain the positions that tend to stick between hope and fear on science and technology — "For those promoting the technologies, such developments hold promises of a better world, for the sceptics they entail Faustian dangers and embody a lot of what is wrong with the modern world" (Hansen, 2010, p. 1) — but to go beyond these polarised positions to further explore the context of political uncertainty, public debate and societal decision-making in which science and technology have been operating (Irwin, 2008).

Moreover, as the particular forms of mediation associated with our six technological settings suggest, the complex interactions between the technology and its users point to an increasing blurring of established ontological and epistemological boundaries that have been used to define humans and nonhumans, their properties and their relations, their abilities and their groupings.

Constitutional legal thinking, however, has traditionally taken for granted the boundary between nature and society, knowledge and norms, as well as the "tacit understanding that humanness is held constant by nature (biology)" (Jasanoff 2011, 10). Indeed, the stability of human nature represents a strong assumption for constitutional documents that should incorporate the most lasting foundational principles of societies. Moreover, most legal scholars still maintain a positivistic attitude towards the relation of science and technology and the law that prevents a proper understanding of current changes.

In contrast, a constructivist approach provides a better account of technoscientific and constitutional evolutions. According to Jasanoff, though the elements of the technoscientific constitutional moment are mostly unwritten, they already reveal some specific features. The traditional separation between science and politics is going to be deeply revised; new forms and forums for deliberation are emerging; technology has become an instrument for governing and control.

First, the challenges that, in the last few decades, life sciences together with ICT have been posing to humanity have both shaken most conceptions of human nature and raised the issue of how to make normative continuity compatible with individual and societal constant change. Technological artifacts are reshaping the dynamics of social order at many levels, from ideas of identity to the boundaries between subjects and objects, to conceptions of liberty, autonomy, and agency (Jasanoff 2003, 6).

Second, the question about whose subjects are legitimately entitled to provoke, and ask for, constitutional changes has been increasingly connected to matters of democracy and participation.

Constitutions represent the most foundational normative moment for democratic societies dealing with technoscientific changes. They appear today as 'spaces' that citizens can factually and symbolically reinterpret as the dynamic epistemic and normative repositories of meaning for human and societal developments.

The twentieth century's politics and ethics that quite paternalistically helped stabilize the biological and genetic revolution are now superseded by "citizens asserting a right to

participate in both the epistemic and the normative evaluation of competing options" (Jasanoff 2011, 295). These tendencies are increasingly taking the shape of dispersed activities of reordering knowledge and society: a re-constitution of the social fabric by citizens for citizens with far-reaching democratic implications (Jasanoff 2011, 295). What Jasanoff argues primarily about citizens' self-reinterpretation of life and rights has de facto merged with similar and even more extended practices through information and communication spaces and devices.

Similar forms of normalization have been performed, both at the public and private levels, to deal with the challenges introduced by life sciences and ICT. In fact, the roles performed by ethics (and ethics committees) in the biological domain—mostly consisting in conveying reassurance about the correct and complete identification and control of potential negative implications—can be compared to what the right to privacy has done for the ICT field—namely certifying that under the umbrella of the private sphere all sensitive aspects of human life would be accounted for, and taken care of. In both cases, a "normative fix" has been constructed as a "technical fix" to avoid deep questioning of the new constitutional dimensions involved by science and technology.

Neither institutionalized ethics nor privacy have accomplished this task satisfactorily, and have faced increasing resistances due both to the complexity of unexpected outcomes, and to higher expectations from citizens towards more democratic forms of governance. Not only rethinking the constitutional dimensions of our lives implies more than just 'listing' the 'ethical implications' of new technologies or protecting individuals' privacy and data, but also requires looking inside the intricacies of knowledge and normativity. This means opening up the epistemic and legal imagination entrenched in new technologies and their architectural structures. It consists in considering values embodied both by our technologies and in making them a site for transparent access and choice. It involves favoring human integrity and agency, preserving it from impoverished human relations, and from unlearning human values. It implies going beyond an atomistic vision of society and supporting a variety of forms of collaboration and cooperation, learning processes, empowerment and usability of knowledge.

Moreover, the deterministic equation between technology and democracy needs to be open to rights and public decisions. Constitutions "are built, they are not found" and do not "magically appear." Similarly there is no reason to think that liberty "in cyberspace will simply emerge." "Left to itself, cyberspace will become a perfect too for control" (Lessig 2006, pp.5-6). And the same can be said of all ICT.

While technology benevolence "must today be argued and won, not simply assumed," looking into ICT architectures and at the values embedded, and opening them up to citizens' rights is building a new generation of rights in design.

As the epistemic and normative codes of life sciences, ICT, and the law mutually constitute themselves, an adequate account of their recursive co-produced interactions is still lacking.

REFERENCES

Beck, U. (2000). Risk Society Revisited. In B. Adam, U. Beck & J. Van Loon (Eds.), *The risk society and beyond - Critical issues for social theory* (pp. 211-229). London: SAGE Publications.

Benkler, Y. (2011). *The Penguin and the Leviathan: How Cooperation Triumphs over Self-Interest*. New York: Crown Business.

Bertolotti, T., & Magnani, L. (forthcoming). A philosophical and evolutionary approach to cyber-bullying: Social networks and the disruption of sub-moralities. In C. Rizza & Â. G. Pereira (Eds.), *Ethics of Social Networks for special need users, Journal of Ethics and Information Technology*: Springer.

Blanchette J.-F., Johnson D.G., (2002). Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness. *The Information Society*, 18, pp.33–45.

Boyd, D. (2006). Friends, Friendsters, and Fop 8: Writing community into being on social network sites. *First Monday, 11*(12). http://firstmonday.org/article/view/1418/1336

Boyle, J. (1996). *Shamans, Software, and Spleens: Law and the Construction of the Information Society*. Cambridge, MA: Harvard University Press.

Broadbent, S., Dewandre, N., Ess, C., Floridi, L., Ganascia, J.-G., Hildebrandt, M. (2013). *The Onlife Initiative* Retrieved from http://ec.europa.eu/digital-agenda/onlife-initiative-0

Calhoun, C. J. (2002). Imagining Solidarity: Cosmopolitanism, Constitutional Patriotism, and the Public Sphere. *Public Culture, 14*(1, Winter 2012), 147-171.

Cammaerts, B., & Van Audenhove, L. (2005). Online political debate, unbounded citizenship, and the problematic nature of a transnational public sphere. *Political communication, 22*(2), 179-196.

Capurro, R., Britz, J., Hausmanninger, T., Nagenborg, M., Nakada, M., & Weil, F. (2011). Editorial: Ethics of Online Social Networks *International Review of Information Ethics (IRIE), 16*(12/2011), 1-2.

Castellanos, C. (2006). *Towards New Bodies and New Biologies: Life as Code, Body as Protocol*. Paper presented at the CODE, Human Systems, Digital Bodies, Conference held at Miami University, Oxford, Ohio. http://www.units.muohio.edu/codeconference/papers/papers/body_bio_protocol_new.pdf

Castells, M. (2010). *The Rise of the Network Society* (2nd ed. Vol. I). Chichester: Wiley-Blackwell.

Chatwin, B, (1987) *The Songlines*, London: Jonathan Cape.

Cocking, D. (2008). Plural Selves and Relational Identity: Intimacy and Privacy Online In J. van den Hoven & J. Weckert (Eds.), *Information Technology and Moral Philosophy* (pp. 123-141). Cambridge: Cambridge University Press.

Coleman, S. (2005). The Lonely Citizen: Indirect Representation in an Age of Networks. *Political communication, 22*(2), 197-214. doi: 10.1080/10584600590933197

Coleman, S., & Blumler, J. G. (2009). *The Internet and Democratic Citizenship: Theory, Practice and Policy*. Cambridge: Cambridge University Press.

Coll, S., Glassey, O., & Balleys, C. (2011). Building social networks ethics beyond "privacy": a sociological perspective. *International Review of Information Ethics (IRIE), 16*(12/2011 - Ethics of Online Social Networks), 45-53.

Crabb, P.B, & Stern, S.E. (2010). Technology traps: Who is responsible? *International Journal of Technoethics*, 1(2), 19-26.

Dahlgren, P. (2004). Foreword. In W. v. d. Donk, B. D. Loader, P. G. Nixon & D. Rucht (Eds.), *Cyberprotest: New Media, Citizens and Social Movements* (pp. XI-XVI). London, New York: Routledge.

P. De Hert, (20089) *A Right to Identity to Face the Internet of Things*, Strasbourg: Unesco. Available at: http://portal.unesco.org/ci/fr/files/25857/12021328273de_Hert- Paul.pdf/de%2BHert-Paul.pdf

European Commission (2006): From RFID to the Internet of Things; Pervasive networked systems. (DG Information Society and Media), 2006, 32p (Available at: ftp://ftp.cordis.europa.eu/pub/ist/docs/ka4/au_conf670306_buckley_en.pdf).

EPIC. (2012). Petition to the FAA: Drones and Privacy.

ERSG. (2013). Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System: Final report from the European RPAS Steering Group: The European RPAS Steering Group.

European Union. (2000). The Charter of Fundamental Rights of the European Union. *Official Journal of the European Communities, C364/3, 18/12/2000*.

FAA. (2013). FAA UAS Online Listening Session. http://www.faa.gov/about/initiatives/uas/media/uastranscription.pdf

Felt, U., & Fochler, M. (2009). The Bottom-up Meanings of the Concept of Public Participation in Science and Technology. *Science and Public Policy, 35*(7), 489-499.~

Flew, T., & Young, G. (2005). *From e-Government to online deliberative democracy*. Paper presented at the International Conference on Engaging Communities, 14-17 August 2005, Brisbane Convention & Exhibition Centre, Queensland, Australia. http://www.engagingcommunities2005.org/abstracts/S101-flew-t.html

GAO. (2013). Unmanned Aircraft Systems: Continued Coordination, Operational Data, and Performance Standards Needed to Guide Research and Development Washigton, DC: U.S. Government Accountability Office.

Gastil, J. (2000). Is Face-to-Face Citizen Deliberation a Luxury or a Necessity? *Political communication, 17*(4), 357-361. doi: 10.1080/10584600050178960

Gottweis, H., & Lauss, G. (2010). Biobank governance in the post-genomic age. *Personalized Medicine, 7*(2), 187-195. doi: 10.2217/pme.10.4

Hansen, M. B. N. (2006). *Bodies in Code: Interfaces with Digital Media*. New York: Taylor & Francis.

Hansen, J. (2010). *Biotechnology and Public Engagement in Europe*. New York: Palgrave Macmillan.

Hildebrandt, M. and Gutwirth, S. (eds.), *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer, Dordrecht.

Howard, P. N. (2005). Deep Democracy, Thin Citizenship: The Impact of Digital Media in Political Campaign Strategy. *The ANNALS of the American Academy of Political and Social Science, 597*(1), 153-170. doi: 10.1177/0002716204270139

Huerta, M. (2012). [Open letter to congressmen].

Irwin, A. (2008). STS Perspectives on Scientific Governance. In E. J. Hackett, O. Amsterdamska, M. Lynch & J. Wajcman (Eds.), *The Handbook of Science and Technology Studies* (3 ed., pp. 583-607). Cambridge, Massachusetts: The MIT Press.

Janssens, A. C. J. W., & Kraft, P. (2012). Research Conducted Using Data Obtained through Online Communities: Ethical Implications of Methodological Limitations. *PLOS Medicine, 9*(10). http://www.plosmedicine.org/article/info%3Adoi%2F10.1371%2Fjournal.pmed.1001328 doi:10.1371/journal.pmed.1001328

Jasanoff, S. (2003). In a Constitutional Moment: Science and Social Order at the Millennium *Social Studies of Science and Technology: Looking Back, Ahead* (Vol. 23, pp. 155-180): Springer Netherlands.

Jasanoff, S. (2011). Conclusion. In S. Jasanoff (Ed.), *Reframing Rights. Bioconstitutionalism in the Genetic Age* (pp. 287-295). Cambridge, Massachusetts: The MIT Press.

Kember, S., & Zylinska, J. (2012). *Life after New Media: Mediation as a vital process*. Cambridge, MA: The MIT Press.

Koch, V. G. (2012). PGTandMe: social networking-based genetic testing and the evolving research model. *Health Matrix: Journal of Law-Medicine, 22*(1), 33-74.

Krochmal, M. (1998). Magaziner, Lessig Spar over Domain Name Plan. *Techweb News, June 11, 1998*. http://www.mail-archive.com/list@ifwp.org/msg06394.html

Latour, B. (1992). Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts. In W. E. Bijker & J. Law (Eds.), *Shaping Technology/Builing Society* (pp. 225-258). Cambridge: MIT Press.

Latour, B. (1993). *We Have Never Been Modern*. Cambridge, Massachusetts: Harvard University Press.

Leiter, B. (2010). Cleaning Cyber-Cesspools: Google and Free Speech. In S. levmore & M. C. Nussbaum (Eds.), *The Offensive Internet: Speech, Privacy, and Reputation* (pp. 155-173). Cambridge, MA: Harvard University Press.

Lenhart, A., & Madden, M. (2007). Social Networking Websites and Teens (pp. 10): Pew Research Centre: The Pew Internet & American Life Project.

Lippmann, W. (1922). *Public opinion*. New York: Harcourt, Brace and Company.

Lunshof, J. E., Chadwick, R., Vorhaus, D. B., & Church, G. M. (2008). From genetic privacy to open consent. *Nature Reviews Genetics, 9*(May 2008), 406-411. doi: 10.1038/nrg2360

Lusoli, W., Ward, S., & Gibson, R. (2006). (Re)connecting Politics? Parliament, the Public and the Internet. *Parliamentary Affairs, 59*(1), 24-42. doi: 10.1093/pa/gsj010

Mannermaa, M. 2007. Living in the European Ubiquitous Society. *Journal of Future Studies*. Vol. 11, No. 4. pp. 105-120.

Mayer-Schönberger, V. (2009) *Delete - The Virtue of Forgetting in the Digital Age*. Princeton, NJ: Princeton University Press.

McGill, J., & Kerr, I. (2012). Reduction to Absurdity: Reasonable Expectations of Privacy and the Need for Digital Enlightenment In J. Bus, M. Crompton, M. Hildebrandt & G. Matakides (Eds.), *Digital Enlightenment Yearbook 2012* (pp. 199-217). Amsterdam: IOS Press.

Mueller, M. M. (2002). *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: The MIT Press.

Newell, B. C. (2011). Rethinking Reasonable Expectations of Privacy in Online Social Networks. *Richmond Journal of Law and Technology, XVII*(4), 1-61.

Nietzsche, F. (1997) *On the Use and Abuse of History for Life*, transl. A. Collins. New Jersey: Prentice Hall.

NTIA. (1998). Management of Internet Names and Addresses. White Paper: Federal Register. 63: 31741.

O'Hara, K., Morris, R., Shadbolt, N., & Hitch, G. 2006. Memories for life: A review of the science and technology. *Journal of the Royal Society Interface* 3: 351–365

Parsell, M. (2008). Pernicious virtual communities: Identity, polarisation and the Web 2.0. *Ethics and Information Technology, 10*(1), 41-56. doi: 10.1007/s10676-008-9153-y

Post, D. (1998). Cyberspace's Constitutional Moment. *American Lawyer,* (November). http://www.temple.edu/lawschool/dpost/DNSGovernance.htm

Rizza, C., & Pereira, Â. G. (2013). Social networks and Cyber-bullying among teenagers: EU Scientific e political report: European Commission, Joint Research Centre: Publications Office of the European Union

Saha, K., & Hurlbut, J. B. (2011). Research ethics: Treat donors as partners in biobank research. *Nature, 478*(20 October 2011), 312-313. doi: 10.1038/478312a

Saha, K., & Hurlbut, J. B. (2012). Opinion: Occupy Science? *The Scientist,* (January, 24). http://www.the-scientist.com/?articles.view/articleNo/31624/title/Opinion--Occupy-Science-/

Skloot, R. (2010). *The Immortal Life of Henrietta Lacks*. New York: Random House.

Stahl, B. C. (2011) IT for a better future: how to integrate ethics, politics and innovation, *Journal of Information, Communication and Ethics in Society*, Vol. 9 Iss: 3, pp.140 - 156.

Stokes, P. (2012). Ghosts in the Machine: Do the Dead Live on in Facebook? *Philosophy & Technology, 25*(3), 363-379. doi: 10.1007/s13347-011-0050-7

Sujon, Z. (2007). New Citizenships? New Technologies, Rights and Discourses. In P. P.-V. Nico Carpentier, Kaarle Nordenstreng, Maren Hartmann, Peeter Vihalemm, Bart Cammaerts and Hannu

Niemenin (Ed.), *Media Technologies and Journalism in an Enlarged Europe* (pp. 201-218): Tartu University Press.

Tallacchini, M. (2013). Human Tissues in the 'Public Space': Beyond the Property/Privacy Dichotomy. In G. Pascuzzi, U. Izzo & M. Macilotti (Eds.), *Comparative Issues in the Governance of Research Biobanks* (pp. 87-104). Dordrecht: Springer.

Thompson, R. M. (2013). Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses: Congressional Research Service

Trottier, D. (2012). *Social Media as Surveillance: Rethinking Visibility in a Converging World*. Farnham: Ashgate.

Turkle, S. (1996). Virtuality and its discontents. *The American Prospect, 7*(24, Winter 1996), 50-57.

Turkle, S. (2011). *Alone Together: Why we Expect More from Technology and Less from Each Other*. New York: Basic Books.

Vallor, S. (2012). Social Networking and Ethics. *The Stanford Encyclopedia of Philosophy.* Winter 2012. Retrieved 10 November, 2013, from http://plato.stanford.edu/archives/win2012/entries/ethics-social-networking

van Dijk, J. (2006). *The Network Society: Social Aspects of New Media*. London: SAGE Publications.

Vesnic-Alujevic, L. (2011). *Political communication on Facebook: A case study of the 2009 European Parliament elections*. Gent: University Press.

Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity Versus Liberty. *The Yale Law Journal, 113*, 1153-1221. http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers

Wicker, S. B., & Santoso, S. M. (2013). Access to the Internet Is a Human Right. *Communications of the ACM, 56*(6), 43-46. http://cacm.acm.org/magazines/2013/6/164596-access-to-the-internet-is-a-human-right/fulltext doi:10.1145/2461256.2461271

Wilsdon, J., & Willis, R. (2004). See-through Science: Why public engagement needs to mode upstream. London: Demos.

Winickoff, D. E. (2006). Genome and Nation. Iceland's Health Sector Database and its Legacy. *Innovations, Spring 2006*, 80-105.

Wojcieszak, M. E., Baek, Y. M., & Carpini, M. X. D. (2010). Deliberative and Participatory Democracy? Ideological Strength and the Processes Leading from Deliberation to Political Engagement. *International Journal of Public Opinion Research, 22*(2), 154-180. doi: 10.1093/ijpor/edp050

Wynne, B. (2007). Public Participation in Science and Technology: Performing and Obscuring a Political–Conceptual Category Mistake. *East Asian Science, Technology and Society: An International Journal, 1*(1), 99-110.

European Commission

EUR 26455 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: **The constitution of the hybrid world**

Authors: Paula Curvelo, Ângela Guimarães Pereira, Philip Boucher, Melina Breitegger, Alessia Ghezzi, Caroline Rizza, Mariachiara Tallacchini, Lucia Vesnic-Alujevic

Luxembourg: Publications Office of the European Union

2014 – 33 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424 (online), ISSN 1018-5593 (print)

ISBN 978-92-79-35149-5 (pdf)
ISBN 978-92-79-35150-1 (print)

doi:10.2788/58678

Abstract

The development and widespread use of information and communication technologies (ICT) are having a profound impact in many aspects of our daily lives, transforming the conditions and procedures of work, changing the modes of communication and social interaction, and altering the fundamental nature of human action, insofar as they play an important role in shaping what we do and how we experienced the world.

In fact, the re-conceptualisation of the very foundational assumptions of modern societies, the new configurations of natural and social life, and the blurring of ontological categories upon which our political, social and legal orders are based, point to fundamental aspects of the human condition that have been reshaped by the hybridisation processes characterising modern human entanglements with emerging technologies. Despite the constitutional nature of these transformations, the basic rules that bind a state to its citizens have undergone small adjustments and accommodations. This not only shows how constitutional rights continue to be regarded as the most stable elements of national life, but also calls attention to the need of looking for the ways in which unwritten and emergent rules of constitutional dimension are being crafted.

Where can we observe the new constitutional order that is emerging at the present moment? What fundamental aspects of human life are being transformed by the mediated role played by new ICT? What are the far-reaching ethical, legal and social implications of these transformations? In what way the most fundamental human rights and the most fundamental relations between states and citizens are being reframed in view of cross-cutting transformations in law and new ICT?

In this paper we propose to address these questions by focusing our analysis on complex forms of mediation and translation that emerge from the use of the Internet and other ICT-based network arrangements.

LB-NA-26455-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle. Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

ISBN 978-92-79-35149-5
doi:10.2788/58678