Redress Procedures in the Digital Sphere

Daniele Santoro

National Research Council of Italy (CNR-IRPPS)

Luiss University, Rome

daniele.santoro@irpps.cnr.it

***

In the recent debate over the rights of agents in the digital sphere, much discussion has ben raised by issues concerning the impact of Big Data over the right to privacy. This debate, originally prompted by the war on terror in the post 9/11 scenario, has recently regained the forefront due to Snowden's revelations on the NSA practices of data collection. The bulk of the debate concerns the use of ICT technologies in accessing digital profiles in order to track information about potential criminal activities, as well as profiling possible terrorists. For many, this form of large scale spoofing and storing of personal information is the only strategy available to acquire intelligence in order to preempt new attacks. As the argument goes, secretive practices are justified by the necessity to strike a balance between the freedoms of citizens and the imperative of national security. In the opposite camp, advocates of privacy rights and civil liberties insist that the intrusive practices of Big Data technologies represent a serious threats to fundamental rights

In this paper I will address two point. First I will explore the impact of this practices on the individual rights in the digital sphere. Second, I will discuss which mechanisms accountability should be enacted in order to protect fundamental rights in the digital sphere.

1. Rights in the digital sphere

By the term 'sphere' I refer to Walzer's concept of those modes of relationship and institutional schemes constitutive of complex societies, such as the political, the economic, and medical sphere, each of which is defined by specific criteria of justice in the distribution of rights, duties, and goods (Walzer 1983). Amongst the different spheres, the digital sphere is most pervasive, for data gathered and exchanged in the online world concern virtually every domain of the social life. But, what does defined the digital sphere? I will argue that the constituent good that defines the domain of the digital sphere is information, or better the exchange of information.[1]

The need to constraint flows of information within the digital spheres is a way to provide more effective means to private citizens over their data against the threat of Big Data phenomena. Attempts in this direction have sought to establish some criteria for

[1] By 'information' I refer to a collection of data semantically structured. More exactly, following Floridi (2010), we can formulate the notion of 'information' as a set of 'well formed' data related by some syntactic rules that govern the system being used in ways that are semantically meaningful, that is can be interpreted within the system.

constraining unrestrained flows of personal data that may affect people also in the offline world. Among the ways people can be affected, Van den Hoven (2008: 310-319) mentions information-based harm, informational injustice (in the Walzer's sense of a violation of complex equality[2]), the exploitation of information (in the markets), and the violation of moral autonomy guaranteed by privacy measures.

Legislative initiative in this direction has taken place at the European level, where the Commission has put forward in 2012 a proposal of reform of the Data Protection Regulation, including the institution of the Right to be Forgotten and the Right to Data Portability.[3] While these measures represent important improvements in the direction of a more substantive protection of individual digital rights, their enactment is still partial, and the new Regulation is not meant to enter into force before the next two years. Moreover, the comprehensive list of measures has not yet been yet decided, and a Directive on this matter is still underway.

2. Redress and accountability mechanisms

In this second part of the paper I will focus on mechanisms of safeguards and accountability superseding the rights in the digital sphere. In particular, I will address the so-called redress procedures that a uniform legislation (such as a Directive) should enforce in cases digital rights are endangered, whether by government or private agencies. In particular, I will explore the argument that, when even when digital rights are limited by institutional agencies due to emergential circumstances (such as national security or public safety), mechanisms of transparency along the lines of freedom of information access, should grant the possibility of an ex-post assessment of the specific use and storage of private data. In discussing this point, I will mainly look at the epistemic aspects of rights (Wenar 2003) and of democratic decision-making (Peter 2008, Estlund 2008).

Cases to this effect include profiling, transfer of data from one sphere of pertinence to another (as in the case of medical data), and collection in bulk. I will argue that we should be particularly careful about regulations allowing open consent to the use of data, and that ex-post measures should in that case grant the right to cancellation and anonymisation of those data. Time allowing, I will explore the justification of acts of 'digital disobedience' (*alas* civil disobedience) against violators when the right to a proper redress is not met.

---

[2] Walzer claims that spheres should be kept separated in order to avoid confusion between the unduly influence one sphere onto the other, and he calls *complex equality* the consideration of which advantages and positions regarding the distribution of a good in one sphere can (or cannot) be converted in advantages in another sphere.

[3] See: http://ec.europa.eu/justice/data-protection/.

References

Estlund, D. M. (2008), *Democratic Authority. A Philosophical Framework*, Princeton University Press;

Floridi, L. (2010), *Information. A Very Short Introduction,* Oxford University Press;

Peter, F. (2008). "Pure Epistemic Proceduralism", *Episteme: A Journal of Social Epistemology* 5(1): 33-55;

Van den Hoven, J: (2008), "Information technology, privacy, and the protection of personal data", In van den Hoven J, Weckert J (eds.), *Information technology and moral philosophy*, Cambridge, New York: Cambridge University Press: 301-321;

Wenar, L. (2003), "Epistemic Rights and Legal Rights", Analysis 63(2): 142-6.