5.2

Is privacy dead? Some reflections by way of an answer

Carlos Gregorio de Gràcia[1]

The first question that needs to be addressed is whether rights can die... and this is not an easy question to answer, at least from a legal point of view. Today we all believe that slavery (as in the right to own another person) is dead. And yet in Brazil, for example, cases of slave labour continue to be filed with the Tribunal Superior de Trabalho. On the other hand, when slavery was abolished in Brazil, a legislative decision was not considered sufficient: the minister of justice at the time, Rui Barbosa, ordered the burning of all written records of slave ownership, in the so-called Queima dos Arquivos da Escravidão.[2] This shows that rights do not only rely upon legal formalities, traditions or the administration of justice; other elements such as databases and other information sources play a significant role in their existence.

Therefore, in order to discuss the potential death of "privacy", we also need to ask how the right to privacy was born. Two different births can be defined. One took place in the United States, with the works of Warren and Brandeis in the 1890s,

1 Researcher and consultant with Instituto de Investigación para la Justicia, Uruguay

2 This incident (the burning of the slavery records), which took place in 1891, regardless of the controversy around its real motives, demonstrates that there is a close relationship between the "records" and rights, between the existence of the former and the validity of the latter, and that it not possible to guarantee certain rights if an active database is maintained, and vice versa. For this reason, it is not enough to look at privacy laws and their implementation; it is also necessary to analyse what personal information is recorded and for what purpose.

dealing primarily with the protection of one's private sexual life. The right to privacy per se is not addressed in the U.S. constitution, and has thus been shaped by the Supreme Court through a series of rulings, most of them handed down on cases related to sexuality, once again. To offer a recent example, a ruling in Vernonia School District v. Wayne Acton et ux. 515 U.S. 646 (1995) considers that athletes have a lesser expectation of privacy precisely due to the degree of public nudity entailed by their participation in sports (in communal locker rooms and showers, for example).

In the meantime, privacy was also born in Europe, but in this case, in the form of the protection of personal information. The underlying motive is a historical event: the extermination of Jews, Gypsies and other specific groups of people undertaken by the Nazis in Germany using census data to identify their victims. From this experience the Germans learned that the only way to protect citizens in the future, in the event of new concentrations of power, was to prevent the accumulation of personal information from the outset. This perception of the protection of personal information as a fundamental right spread throughout Europe.

It is therefore not surprising that the first Latin American law on the protection of information was adopted in Argentina in 1994 as a consequence of the inclusion of habeas data in a constitutional reform. Links could be drawn between the personal information protection movement in Argentina and the extermination practices of the military dictatorship (1976-1985). Not only did the military regime make use of the personal information gathered in the name of "state intelligence"; in addition, when individuals were captured, their telephone and address books were used to identify, investigate and capture the contacts listed in them.

From an information society perspective, the U.S. paradigm of privacy has lost relevance, because sexuality is no longer the taboo subject it was in 1890, and sexual issues are publicly addressed without a great deal of censure.

At the same time, the perception of the protection of personal information as a fundamental right as conceived by the European tradition is better suited to dealing with the problems of the information society. In the face of massive flows of sensitive information with no type of control or protection, the main risk that needs to be avoided is discrimination for unjust purposes.

This can be seen through a careful study of the most recent legislation on the privacy of health information in the United States,[3] which, we could say, has adopted the European paradigm of the protection of personal information and left far behind the concept of the right to be let alone of the traditional U.S. approach to privacy.

From the European perspective, the protection of information is one of the rights encompassed by the freedom of expression. This freedom includes first and foremost the right to express oneself, but it also includes the freedom of non-expression (also called informational self-determination, which is tantamount to the right to protection of personal information), as well as the freedom of audience. The implications of free speech can be addressed from either a "speaker-focused" or "audience-focused" perspective. The freedom of audience is concerned with offering citizens greater access to conflicting viewpoints and non-mainstream subject matter, not only because those with "disruptive" ideas have the right to be heard, but also because society has a special interest in hearing them. This updated view of the freedom of speech does not reinforce the right to express "eccentric" ideas, but rather places priority on the right of all citizens to have access to all ideas, and especially to those that do not coincide with their own way of thinking.

When we analyse current threats, it is evident that privacy and the protection of personal information are under attack, but they cannot die, because without these rights we would

3 See Privacy Act 5 U.S.C. § 552a, 45 CFR 160.103, Subpart E—Privacy of Individually Identifiable Health Information § 164.501 and in particular HITECH Act TITLE XIII- Subtitle D—Privacy - SEC. 13400

be much more vulnerable to discrimination (in access to employment, credit, insurance, health care, etc.) with no means of protection.

In the context of the current development of the information society, a number of rights are critically endangered. First of all, the right to anonymity and anonymous speech, since the enormous amount of data in circulation has given rise to the emergence of mathematical algorithms that can be used to "de-anonymise" data. Studies on databases of medical prescriptions have found that the probability of de-anonymising patient data based on a postal code and date of birth is 69%, and if the patient is over 60 years of age, that probability rises to 95%.[4]

Freedom of speech is also endangered. While it may be possible to express oneself more freely, it is difficult to access differing opinions, because the tendency is to follow known figures, while the views of unknown figures remain relatively inaccessible. In this regard, the so-called Google filter bubble infringes on the freedom of speech from an audience-focused perspective: search results are presented according to criteria based on previous searches, which means that alternative viewpoints may be left out.

The protection of personal information is also at risk, not necessarily due to technological developments, but rather as the result of legal decisions in both Europe and the Americas, where the classification of data as protected or unprotected is justified on the basis of a "predominant public interest". In 2001, the Privacy Commissioner of Canada determined that the name of a physician on a medical prescription does not qualify as protected personal information. In a similar vein, the U.S. Supreme Court ruled that free access to the names of physicians is justified by legitimate corporate interests.[5] These decisions

4 Sweeney, L. 1997. "Weaving Technology and Policy Together to Maintain Confidentiality". *Journal of Law, Medicine & Ethics, 25, nos. 2&3*: 98-110 www.dataprivacylab.org/dataprivacy/projects/law/jlme.pdf

5 Sorrell v. IMS Health Inc., 23 June 2011

served to expand the already established concept of public figures –and their consequent loss of privacy– to partially public figures, a category which could be extrapolated to include all professionals in the exercise of their professions.

In Latin America, the right to the protection of personal information has followed the European route in Argentina, Uruguay, Mexico, Peru, Colombia and Costa Rica. In other countries, laws are still evolving. Agencies for the protection of personal data in the region are still very weak. In Argentina, for example, only 25 fines have been imposed during the more than 12 years that the law has been in force, while in Spain there can be this many fines in a single day. Ironically, the adoption of data protection laws in the Latin American region was motivated more by the desire to tap into the call centre market[6] than to ensure respect for a fundamental right (with the possible exception of Mexico and Colombia).[7]

While attacks on personal information can come from both the state and from private companies, those from companies are more dangerous. Some would argue against this statement, primarily because states handle sensitive information on their citizens. However, there is a qualitative difference, namely the existence of laws on access to public information. In Latin America –with the exception of Argentina– and particularly in Mexico, access to information laws pre-dated data protection laws, and have provided citizens with the opportunity to know what information is in the state's possession. Consider, for

6 There are studies that link the expansion of the call centre market in Argentina to its certification by the European Commission as providing an "adequate level of protection" for personal information (Decision 2003/490/CE). Since the operations of offshore call centres (for example, when calls made by users in Europe are forwarded to customer service agents in Argentina) involve the handling of personal information, a declaration of equivalent legislation would provide users with a guarantee of the protection of that information.

7 Remolina, Nelson. 2013. "41 personas condenadas por el delito de violación de datos personales y 544 multas por infracción de la ley 1266 de 2008" 18-04-13 *Observatorio Ciro Angarita Barón* www.habeasdatacolombia.uniandes.edu.co/?p=980

example, the destruction of the RENAUT (National Registry of Mobile Telephony Users) database in Mexico, ordered by the Federal Institute for Access to Information and Data Protection to protect the privacy of mobile users.[8] Paradoxically, since 2003 there has been a law in force in Argentina establishing free access to environmental information which includes private companies.[9] In many cases, people are unaware of how much information on them is in the possession of companies, and how and for what purposes that information is being used. If there is no authority responsible for guaranteeing the protection of personal information, and if exemplary financial penalties are not imposed, it is unlikely that any company will change its policies.

Ultimately, the protection of privacy and personal information is not dead, but it does need to be revitalised. This will require efforts to raise awareness among citizens regarding how necessary these rights are for their daily lives, and among the authorities regarding respect for human rights and the rule of law.

8 "Destruye Segob bases de datos personales del Renaut" 15-06-2012 *Proceso* www.proceso.com.mx/?p=311021

9 República Argentina. *Ley 25.831 Régimen de libre acceso a la información pública ambiental.* www.infoleg.gob.ar/infolegInternet/anexos/90000-94999/91548/norma.htm