Chapter 22
Oblivion Is Full of Memory:
Legal Issues Raised in the EU by the Right to Erasure

Anabelen Casares Marcos
Universidad de León, Spain

ABSTRACT

The right to informational self-determination has raised bitter debate over the last decade as to the opportunity and possible scope of the right to demand withdrawal from the internet of personal information which, while true, might represent a detriment that there is no legal duty to put up with. The leading case in this topic is that of Mario Costeja, Judgment of the EU Court of Justice, May 13, 2014. The interest of recent European jurisprudence lies not so much in the recognition of such a right but in the appreciation of certain limits to its implementation, assisting data protection authorities in balancing the rights at stake in each case. Reflection on the current status of the issue considers rights and duties imposed in the matter by Regulation (EU) 2016/679, of 27 April, known as the new General Data Protection Regulation.

INTRODUCTION: DATA PROTECTION RIGHTS AS PATH TO INFORMATIONAL SELF-DETERMINATION

Unstoppable innovation leads to new exciting technological challenges, such as those posed by the Internet of Things (IoT), Augmented Reality (AR), Cloud or Edge Computing, the deployment of 5G, the expansion of WiFi 6, investment in advanced data analytics, machine learning from Artificial Intelligence (AI) and Machine Learning, Blockchain, Conversational AI tools, Always-Connected-PCs (ACPC) or Robotic Process Automation (RPA). Their almost unlimited potential to collect and process personal data unleashes an irrefutable threat questioning the capacity of the citizens of the 21st century to control all the personal information on the internet that refers to them or that somehow affects them.

Not surprisingly, the so-called information society is marked by a constant technological renewal since the second half of the 20th century, which has even led to debate on whether the label itself should

DOI: 10.4018/978-1-7998-5728-0.ch022

be considered superseded and replaced for that of knowledge society (Bello, 2005; Toniatti, 1991). The latter is not just mere access and exchange of information and data, as "knowledge is information structured in representations, integrated, relevant, aimed at *interpreting* data (through schemes and models), *explaining*, *foreseeing*, usable in effective action or in thinking" (Castelfranchi, 2007). The recent Communication from the Commission, *Shaping Europe's digital future*, COM (2020) 67 final, firmly states that "digital technologies are profoundly changing our daily life, our way of working and doing business, and the way people travel, communicate and relate to each other. Digital communication, social media interaction, e-commerce, and digital enterprises are steadily transforming our world. They are generating an ever-increasing amount of data, which, if pooled and used, can lead to a completely new means and levels of value creation. It is a transformation as fundamental as that caused by the industrial revolution."

The legal protection of personal data has therefore been revealed as a fundamental issue in our days for the protection of citizens' rights and freedoms. Even more so if we consider that this continuous technological advance is joined by the futility of solutions articulated independently from other responses tested successfully in the international arena, since there is no doubt that the globality of risks experienced in this area by citizens do not know borders (Piñar, 2008, p. 40). They are, in any case, expected aggressions in the current socioeconomic context, in which information is clearly an instrument of power, unleashing heavy data traffic very difficult to control.

The recognition of the protection of personal data as a fundamental right has been controversial in the international arena, raising exciting doctrinal debates that have helped to clearly define essential concepts as close to each other as, for example, those of intimacy and privacy, ultimately leading to the articulation and confirmation in the EU of a genuine right to informational self-determination (Agúndez, 2010). Emphasizing the radical difference between both, the former is considered broader than the latter, since intimacy protects the sphere in which the most singularly reserved facets of the person's life are developed -the home where daily life is carried out, communications, for example- while privacy constitutes a set of broader and more global facets of the personality that isolated may lack intrinsic meaning but coherently linked cast a portrait of the personality that the individual has the right to keep reserved. The so-called data protection right, originally of eminently jurisprudential creation and definition in the EU, takes privacy as an essential reference for its construction as a true autonomous and independent fundamental right (Guichot, 2005; Martínez, 2004; Piñar, 2008).

While the right to privacy seeks to protect against any invasion that may be carried out in that area of personal and family life that the person wishes to exclude from the knowledge of others and the interference of third parties against their will, the fundamental right to data protection attempts, instead, to guarantee a power of control over personal data, its use and destination, with the purpose of preventing its illicit traffic. Its different scope also allows the holder different possibilities in each case. Thus, the uniqueness of the right to data protection also derives from the fact that it confers on its owner a bundle of legal powers imposing on third parties legal duties such as the right to require prior consent for the collection and use of personal data, the right to be informed about its destination and use and the right to access, rectify and cancel it, in short, the power to dispose of one's personal information. Hence, the right to data protection is also known as the right to informational self-determination, since it guarantees a power of control by citizens over their personal data (Tornos, 2008; Troncoso, 2009).

The problem, as has already been stated, goes far beyond the borders of each specific State to be considered globally, in line with the universal nature and absence of borders of the internet. The attention given to the matter by the EU is not, therefore, surprising. EU regulations ensure a minimum standard of protection of personal data common to all member countries. This purpose has been reinforced after the