Chapter 5
Data Retention and Security in Europe:
Towards a New Right to Digital Privacy

Clara Marsan Raventós
Open University of Catalonia, Spain

ABSTRACT

This chapter describes today's environment of telecommunications data, one where a permanent tension between security, on the one hand, and privacy, on the other, are in a fragile equilibrium. Against this background, the chapter explores the contours of a new right to digital privacy in Europe, a right that belongs to one's personal development and freedom. Firstly, it looks at how it has been jurisprudentially conceived in Germany (in particular through the two recent cases on "on-line searches" [2008] and on the law implementing the Data Retention EC Directive [2010]). Secondly, it explores how this acquis on the right to digital privacy is increasingly present in other member states. Finally, it will be argued that an international agreement on the right to digital privacy should be put in place through the concurrence of all private (ITs) and public stakeholders involved. The latter should agree on the minimum content of this right, as well as on the different channels to enforce it (through legal remedies but also other mechanisms such as "privacy by design").

INTRODUCTION

New technologies provide plenty of opportunities to improve people's lives in diverse domains such as health, work or social life. New technologies, though, can also endanger human rights. Looking at the particular area of personal data and new technologies, we have experienced a tremendous shift on the purposes for which legislators could regulate data management. Traditionally in Europe, data has been regulated in order to protect their use by third parties. Now, instead, regulations tend to address the need to make such data available to third parties. The justification for such a

DOI: 10.4018/978-1-4666-0891-7.ch005

shift has been quite pervasively the fight against crime and, particularly, against terrorism. Here, one can see the double facet of new technologies mentioned above. On the one hand, controlling the data generated and communicated through new telecommunication technologies provides police and intelligence agencies with a powerful weapon to fight the organized crime (Aquilina, 2010). Not only does monitoring telecommunication technologies allow tracing the identity, location, or connection between criminals, but, in fact, today, many crimes are committed through new technological devices. On the other hand, to have police and intelligence agencies digging in telecommunications data as much as they want, highly compromises the right to privacy of individuals. Moreover, while criminals will be prevented to continue with their offences thanks to the law enforcement control of telecommunications traffic, who will control the latter to refrain from seriously encroaching the privacy of individuals? Finally, there must be bored in mind that the control of personal data is not only in the hands of police agencies but, primarily, in those of telecommunication companies for they are responsible for the collection of an enormous amount of private data generated via telecommunications technologies.

Here lies one of the deepest problems in managing the amounts of private data generated in the use of telecommunication technologies; while telecommunication technologies are useful in different domains (i.e. the fight of crime, socializing, communication, etc.) the personal data generated by its use is likely putting at stake core values of the democratic state. The balance that has to be struck between, on the one hand, the access to telecommunication data for law enforcement agencies and, on the other, the respect of the right to privacy is a difficult one. In Europe there has been legislation and jurisprudence at a regional level (CoE and EU) and at a state level that has highlighted that the balancing is not easy and that the stakeholders involved in telecommunication processes should join efforts in order to facilitate that the two different goals of a democratic state—freedom and security as basic human rights—will be equally achieved.

The purpose of this chapter is to analyze the different goods that need to be considered in this balancing through the rich German jurisprudence on privacy and data retention legislation. Moreover, this chapter proposes to develop an independent right to digital privacy (at a national, regional, and international level) in order to provide a minimum of protection to the right to privacy in today's technological world.

TELECOMMUNICATIONS DATA RETENTION IN THE CRUCIBLE OF SECURITY

Background on the Balancing between Security and the Right to Privacy

Since the fight against terrorism has become a ubiquitous topic in today's globalized world, it has been easy to fall into the "anti-terrorism trap" and accept restrictions of rights and liberties—such as the new European data retention framework is *vis-à-vis* the right to privacy—as a necessary answer to terrorism. Klaus Günther had already warned us about the nature of the state in today's globalized world, the purpose of which is to provide security to the consumer-citizen (Günther, 2005, p. 389). If the "anti-terrorist" argument through Günther's reasoning explains why security has taken up on some rights and liberties in most democracies, there are particular examples in the terrain of the fight of terrorism that endorse the argument by which terrorism cannot justify these rights and liberties restrictions. To begin with, terrorism is unfortunately not a new phenomenon in Europe; all European states that had to face terrorism have regulated it without the need to retain all data traffic available. Secondly, at an international and European level there were