Chapter 1
Responsibility, Jurisdiction, and the Future of "Privacy by Design"

Ugo Pagallo
University of Turin, Italy

ABSTRACT

This chapter focuses on some of the most relevant issues in today's data protection: responsibility and jurisdiction are examined in the light of the principle of "privacy by design." On one hand, both from the substantial and procedural points of view, national legal systems determine differently rights and duties in the field of data protection. On the other hand, these divergences can be overcome to some extent, by preventing privacy infringements through the incorporation of data protection safeguards in information and communication technologies. Although it is unlikely that "privacy by design" can offer the one-size-fits-all solution to the problems emerging in the field, it is plausible that the principle will be the key to understand how today's data protection-issues are being handled. By embedding privacy safeguards in places and spaces, products and processes, such as Information Systems in hospitals, video surveillance networks in public transports, or smart cards for biometric identifiers, the aim should be to strengthen people's rights and widen the range of their choices. On this basis, we can avert both paternalism modelling individual behavior and chauvinism disdaining different national provisions of current legal systems.

INTRODUCTION

Although lawyers may disagree on whether we are in the midst of an "information revolution" (Bynum, 2009; Horner, 2010), most of the time they admit that both the internet and computer networks have deeply changed contemporary legal systems. As stressed by several contributions to *Information Technology Law* (Bainbridge, 2008; Lloyd, 2008; etc.), such a profound transformation has affected not only the substantial and procedural sides of the law, but its cognitive features as well. The impact of technology on today's

DOI: 10.4018/978-1-61350-132-0.ch001

legal systems can be fully appreciated through a threefold perspective.

First, technology has engendered new types of lawsuits or modified old ones. As, for example, the next generation of offences arose within the field of computer crimes (*e.g.*, identity thefts), technology impacted on traditional rights such as copyright (1709) and privacy (1890), turning them into a matter of access, control, and protection over information in digital environments (Heide, 2001; Tavani & Moor, 2001; Ginsburg, 2003; Floridi, 2006).

Secondly, technology has blurred traditional national boundaries as information on the internet tends to have a ubiquitous nature. This challenges the very conception of the law as enforced through physical sanctions in the nation-state. Spamming, for instance, offers a good example: It is transnational par excellence and does not diminish despite harshening criminal laws (like the *CAN-SPAM Act* passed by the U.S. Congress in 2003). No threat of sanctions, in other words, seems to limit spamming.

Finally, technology has deeply transformed the approach of experts to legal information. As Herbert A. Simon pointed out in his seminal book on *The Sciences of Artificial*, this transformation is conveniently illustrated by research in design theory, which "is aimed at broadening the capabilities of computers to aid design, drawing upon the tools of artificial intelligence and operations research" (Simon, 1996). While scholars increasingly insist on the specific impact of design or "architecture" and "code" on legal systems (Lessig, 1999; Katyal, 2002; Zittrain, 2008; van Schewick, 2010), both artificial intelligence and operations research not only further design but, in doing so, affect the structure and evolution of legal systems (Pagallo, 2007; Yeung, 2007).

These three levels of impact have, nonetheless, led some scholars to adopt a sort of techno-deterministic approach, leaving no way open to shape or, at least, to influence the evolution of technology. It is enough to mention that some have announced "The End of Privacy" (Sykes, 1999), "The Death of Privacy in the 21st Century" (Jarfinkel, 2000), or "Privacy Lost" (Holtzmann, 2006). On this reading, technology would allow these scholars to unveil an already written future: While, in digital environments, spyware, root-kits, profiling techniques, or data mining would erase data protection, FBI programs like Carnivore or some other means like RFID, GPS, CCTV, AmI, or satellites, would lead to the same effect in everyday (or analog) life. However, strongly decentralized and encrypted architectures providing anonymity to their users, as well as systems that permit plausible deniability and a high degree of confidentiality in communications, suggest that rumours of the death of privacy have been greatly exaggerated. Techno-deterministic approaches are in fact liable to the same criticism that John Kenneth Galbraith put forward in his own field: "The only function of economic forecasting is to make astrology look respectable". In order to provide a more balanced picture of the current state-of-the-art, this chapter examines two of the hottest legal topics in data protection, namely, online responsibility and jurisdiction, which are then analyzed in connection with today's debate on the idea of embedding data protection safeguards in ICT and other types of technologies, that is, the principle of "privacy by design". The goal is to shed further light on the aforementioned threefold level-impact of technology on contemporary legal systems, taking leave from all sorts of techno-deterministic drifts. Accordingly, the chapter is presented in five sections.

First, the *background of the analysis* sums up the claims of "unexceptionalism". In its substantial form, it vindicates the analogy between cyberspace and the "real world," that is, between digital and traditional boundaries of legal systems. In the phrasing of Allan R. Stein, "*The Internet is a medium*. It connects people in different places. The injuries inflicted over the Internet are inflicted by people on people. In this sense, the Internet is no different from the myriad of