 ABOUT THE SUBJECT

In the digital age, ICT raise new concerns that are not accounted for within the existing data protection/privacy legal framework, so some action is therefore necessary to ensure individual rights. After providing an overview of ICT as a new development that creates opportunities and also risks, this book discusses the need to integrate, at a practical level, data protection and privacy from the very inception of new information and communication technologies.

Information and communication technologies (ICT) are enabling tremendous capabilities in virtually every aspect of our lives—how we work, play, socialize and educate. They are essential for today’s information economy and for society in general. ICT have been compared to other important inventions of the past, such as electricity. While it may be too early to assess their real historical impact, the link between ICT and economic growth in developed countries is clear. ICT have created employment, economic benefits and contributed to overall welfare.

The impact of ICT goes beyond the purely economic, since it has played an important role in boosting innovation and creativity. But individuals should be able to rely on ICT’s ability to keep their information secure and control its use, as well as be confident that their privacy and data protection rights will be honored in the digital space.

MISSION AND OBJECTIVES OF THIS BOOK

The mission of this book is to provide comprehensive coverage of the latest and most relevant knowledge, developments, solutions and practical approaches related to this topic that are able to transform society and the way we live from a technological, legal and ethical perspectives.

Some of the most significant objectives of this book include:

- to overcome the fragmentation of knowledge concerning the latest developments on the theme and document the most impact contributions, from legal and regulative developments to its concrete applications, from the discussion of frameworks, approaches and models, to its impact on society and organizations, from technology to people.
- to incentive and to support future trends for research and development
- to discuss advantages, opportunities, challenges, results and future trends
- to support for higher education courses.
The resulting publication is a valuable and multi-faceted resource that gives the reader good insight about where technological developments and legal aspects are taking us in this emerging and more and more relevant expanding domain.

**ORGANIZATION OF THE BOOK**

This book is a compilation of 27 contributions that discuss several dimensions: Information and Technology law and regulation, Knowledge and Information Society aspects related to protection and access rights both for individuals and digital contents, and accessibility issues related to ethics, regulation and standards.

These 27 chapters are written by 68 authors from academe, industry and professionals, related to the different dimensions of the book’s theme: from law to ICT experts, including policy makers.

*Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues* is organized in five sections:

- **Section 1:** ICT Law and Regulation discusses implications, challenges, barriers and opportunities of the Information Society and ICT, namely the legal aspects in the field of intellectual property rights, conflict resolution in electronic commerce and electronic transactions, authentication of digital contents.
- **Section 2:** Policies, Models, Frameworks and Rules introduces new practices, new models and new approaches to data security, to information and knowledge sharing and to collaborative processes.
- **Section 3:** Protection of privacy and trust is concerned with unauthorized accesses to sensible digital information, privacy rights and trust and presents tools and techniques to prevent or control these aspects.
- **Section 4:** Access Rights discusses both web accessibility legislation and standards, and legal aspects of access to digital contents and intellectual property rights.
- **Section 5:** ICT Ethics discusses legal, privacy and security aspects related to ICT ethics in the information and knowledge society.

The first section, ICT Law and Regulation, discusses implications, challenges, barriers and opportunities of the Information Society and ICT, namely the legal aspects in the field of intellectual property rights, conflict resolution in electronic commerce and electronic transactions, authentication of digital contents. This section includes the 14 chapters summarized below.

The Data Retention Directive (2006/24/EC) provides the obligation for providers of publicly available electronic communications services or of public communications networks to retain traffic and location data for six months up to two years for the purpose of the investigation, detection and prosecution of serious crime. In the regulatory framework imposed by this Directive, the Portuguese Law no. 32/2008, of 17 July, requires that providers of publicly available electronic communication services or of public communications networks retain specific communication data, so that such data can be accessed by competent authorities, exclusively for the purpose of investigation, detection and prosecution of serious crime. Retained (via digital storage) metadata of telecommunications acts change and transform into the content of something else: a surveillance program. The concept of a data space that provides movement within and between data described here illustrates the powers of data retention in an imaginable way.
Considering potential uses and misuses of retained data such as traffic analysis, social network analysis and data mining, the first chapter of this book examines the degree of interference with the right to privacy posed by the data retention laws.

In the second chapter, "Information Agents, Social Web and Intellectual Property," the authors argue that due to the development of the information society, there has been a substantial change in regulating certain legal aspects in the field of intellectual property. Focusing on the Internet, there is the need to protect, on the one hand, user interests in use and private access to information in order to ensure security and protection of the data exchanged on the Web and, on the other hand, to ensure respect and protection of copyright of the work as well as the sui generis right of database makers. The picture is extremely complicated as interests and rights that may collide with each other must be combined. In the case of Internet access to different content that is offered on the Web, there is also another problem. In many cases we are not only faced with the problem of determining who owns the rights or who is the author, but a new way of creating content through collaboration or automated software agents is spreading that is radically different from the traditional model which makes it even more complicated to establish the intellectual property regime and the rights derived thereof, as we will understand in the first chapter.

The growing use of telematic ways of communication and of the new developments of Artificial Intelligence brought along new ways of doing business, now in an electronic format, and requiring a new legal approach. Thus, there is an obvious need for legal changes and adaptations, not only concerning a new approach of traditional legal institutes, but also concerning a need for new developments in procedural means. Transactions are now undertaken in fractions of seconds, through the telematic networks, requiring more efficient ways for solving conflicts; on the other hand, the fact that we must now consider commercial transactions totally undertaken within an electronic environment ("online transactions") leads to an obligation of rethinking the ways of solving disputes that will inevitably arise from electronic commerce. Chapter 3, "Conflict Resolution in Virtual Locations" discusses a whole new evolution towards a growing use not only alternative dispute resolution, but also, towards the so-called on-line dispute resolution.

As discussed in the fourth chapter, "Legal Ontologies in ICT and Law," re-usability is frequently declared as sine qua non feature of modern ontology engineering. Although thoroughly examined in general theory of knowledge management models the re-usability issue is still barely a declaration in the domain of legal ontologies. The similar situation also applies to statute-specific ontologies. Those knowledge modeling entities are well described especially as an opposition to the general application legal ontologies. Yet it is trivial to say that most of the developed legal ontologies so far are those generic ones. And this sole fact should not surprise as the very specialized knowledge models – usually harder to develop – are at the same time narrowed with their utility. Of course in terms of re-usability, this simply means that this feature may be largely disabled in this kind of knowledge models. In this chapter the authors face both challenges—by presenting the most interesting trends and works in the field, the authors demonstrate the practical approach to modeling copyright law case by re-using statute-specific ontologies.

According to the authors of chapter 5, "Certified Originality of Digital Contents by the Time Authentication," in our modern clock-ruled culture, it is not too much to say that no society can exist unless based on “time.” Computers, which are the key device of an information society, are equipped with high precision clocks to synchronize their entire circuit function. In an electronic environment or digital society built on computers, recordkeeping relates inevitably to the time that is ticked away by the clocks embedded in the computers. Time is thus the infrastructure of this information society. To save the situ-
ration, a notion of time for the digital society should be properly defined and popularized, specifying the way and conditions of using it safely. The scope of discussion here focuses on some specific industries and applications for time-stamping technologies. The study presented here will be further refined step by step as its validity is verified in actual use. Meanwhile, authors are planning to work on this study for standard time distribution, which is as important as time-stamp to time business.

Chapter 6, “Antitrust Applied to ICT: Granting Access, Promoting Consumers’ Welfare and Enhancing Undertakings’ R&D Investments” analyses how Antitrust is applied to ICT in order to grant access to so-called “essential facilities,” promote consumers’ welfare and enhance R&D investments. Our contentions are underscored by the recent Microsoft ruling. First, the authors summarize the basic principles underlying Article 82 EC Treaty, and the way in which European antitrust authorities are trying to “reshape” it in order to achieve a more economic understanding of abusive practices, specifically refusals to deal. The authors focus on the protection of IPRs, essential to the pivotal role ICT plays in our modern and developed world, and—closely linked to it—the consequences of this landmark case in incentives for innovation and investment. In addition to these, there is the always-present concern for consumers’ welfare, which has become the cornerstone for antitrust decisions and is also addressed here.

The novelty of “new realities” such as Virtual Worlds presents a challenge to the law. Many transactions are made every day on Virtual Worlds, but no taxation is applied to them. Chapter 7, “Taxation of Virtual Worlds: An Approach to Face Virtual Worlds as Electronic Commerce” argues, firstly, that the object of such transactions is subject to the right of property and secondly, that the electronic currency used to buy such property is electronic money. For both conclusions, one important issue considered will be the legal strength of the EULA. The issues of property and electronic money form the basis of this approach to VW taxation. It is argued that virtual transactions should be taxed, and that is possible to create a legal solution that does not endanger the principal of taxing only profit, and does not tax mere entertainment. Tax law must be applied to these transactions. The author considers these two issues, which allow us to view VW as an electronic commerce marketplace.

Support for research and development in information technology is considered today as critical by most governments in industrially advanced countries. Traditionally, the way of stimulating research has been to ensure to the investor the appropriability of the returns generated. Such appropriability is typically implemented by means of Intellectual Property Rights. Nevertheless, the protection of such rights is heterogeneous worldwide. Today, two different legal systems for the protection of software coexist: the system of patents and the system of author’s copyrights. In chapter 8, “Intellectual Property Systems in Software,” the authors explain these two main systems of intellectual property to provide legal protection for software, including the licenses to transfer rights on software. The end of the chapter presents the most recent trends of the EU to replace the current European software protection system, including a discussion on software patents and legal initiatives on the subject. In addition, legal issues linked with trends in software commercialization are presented.

The price of privacy intrusion and security breaches is often due to the ubiquitous connectivity of networks. National entities as well as other governing bodies have passed laws and regulations to assist individuals in their quest to protect their information as it is being transmitted and received over these networks. An international perspective of information privacy and security laws and regulations can provide an insightful view concerning how each country differs as well as the important drivers for these differences. Policy makers can learn from the comparisons made in relation to similarities and differences between privacy and security laws. In chapter 9, “A Global Perspective of Laws and Regulations Dealing with Information Security and Privacy,” the authors have selected different countries
and regions around the world due to the growth of security and privacy threats over the past 10 years as well as their legislative practices.

As discussed in chapter 10, “Intellectual Property Protection and Process Modeling in Small Knowledge Intensive Enterprises,” knowledge-based assets, intellectual property, and capital play a fundamental role in an enterprise’s competitiveness, especially in small knowledge intensive enterprises. Small knowledge intensive enterprises need to create new ways of operating in order to manage the intellectual and knowledge-based assets in their organizations more efficiently. Organizational knowledge and intellectual property can be protected, either formally via IPR, or informally via efficient knowledge management. Successful IP protection requires systematic intellectual property and knowledge management. Intellectual property protection via efficient knowledge management affects the entire organization rather than being just a separate task. It needs to be embedded in organizational work routines, practices, and processes as an overall operational strategy. When embedded in organizational work processes, IP protection and knowledge management become a continuous part of work routines and tasks in the enterprise, not a separate action.

Pervasive computing aims to saturate ambient environments with sensors and processors; affective computing aims to infer emotive and intentional states from physiological readings and physical actions. The convergence of pervasive and affective computing offers genuine promise for creating ambient environments which (re-)configure themselves according to user’s emotive states. On the down-side, there is a real risk of privacy invasion if emotions, behaviours, and even intentions are recorded and subject to the same content-access rules as telephone calls, IP logs, and so on. Based on an experiment to enhance Quality of Experience (QoE) in a visit to a public collection enhanced with pervasive and affective computing, chapter 11, “Privacy in Pervasive and Affective Computing Environments” discusses the subtle interactions and requirements of enhanced service provision vis-à-vis privacy rights. The outcome will contribute to the discussion on ensuring an effective relationship between technologists and application developers on the one hand, and those concerned with privacy rights, ethical computing and formulation of social policy on the other, to promote and protect the rights and interests of citizens.

Inter-systemic contracting may be based upon autonomous intelligent behaviour. Autonomy is an important advantage of software agents. Yet, it brings along several issues concerning the legal consideration (e.g. legal personality/attribution) and the legal consequences of software agent’s behaviour. The intervention of software agents in corporate bodies and the consideration of its roles must also be referred. All this intends interactions based on contracts and relations of trust, at an individual, at a community and at a systemic level. In this regard, it does make sense to speak of the relation between good faith and trust in inter-systemic contracting. And at the systemic level there is a need to focus on special protocols intended to enhance trust in electronic commerce. Chapter 12, “Agents, Trust and Contracts,” proposes smart contracts as a way of enhancing trust and of achieving enforcement in electronic contracting.

As a reaction to the challenges of digitization, recent developments in international copyright law are characterized not only by its strengthening and proliferation but also by the protection of technological protection measures against circumvention acts. Consequently, in the digital context, copyright is being deconstructed and converted into a mere access right to legally and technologically protected information. Considering that copyright must represent a compromise between holders’ and users’ interests, the desired balance has been lost to the disadvantage of the users, potentially harming fundamental and human rights such as freedom of expression and freedom of access to information. In chapter 13, “Between Scylla and Charybdis: The Balance between Copyright, Digital Rights Management and Freedom of Expression,” the author describes the conflict between copyright and freedom of expression, how the
classic compromise achieved by the conflict’s internalization within copyright law and the provision of copyright exemptions may no longer exist and how the users tend to find legal protection externally, outside copyright law.

The objective of chapter 14, “Analysis of Benefits and Risks of E-Commerce: Practical Study of Spanish SME,” is the study of the art of e-commerce, analyzing the different existing commercial models in the market such as Business to Business (B2B), Business to Consumers (B2C), Business to Business to Consumers (B2B2C), Consumers to Business (C2B), Business to Employee (B2E), Administration to Business/Consumers/Administration (A2/B/C/A), Consumers to Consumers (C2C), Peer to Peer (P2P), Mobile to Business (M2B) and Small Office Home Office (SOHO) amongst others, the level of implementation in the workplace as well as the level of acceptation in society and the regulatory framework for the development of the activity. After this study, the central theme will be one of carrying out a study of the pros and cons that e-commerce brings to the client and to the company. Moreover, a study on the implementation of e-commerce in a Small and Medium Enterprise (SME) is conducted, analyzing the technological possibilities and the market of the company which is the object of the study, as well as the associated barriers and risks.

The second section, “Policies, Models, Frameworks and Rules,” includes five chapters that introduce new practices, new models and new approaches to data security, to information and knowledge sharing and to collaborative processes.

Business intelligence is the most powerful part of enterprise information systems (ERP). It is shown in chapter 15, “Data Security Legislative as Data Shredding Mill,” that the absence of the counterpart of business intelligence in e-government called civic intelligence (CI) has important negative consequence that are probably more severe than the absence of business intelligence for enterprises. Missing CI threatens the prosperity of countries and nations as it has crucial negative effects on social processes like the quality of education, healthcare research, and research and control of economic processes. Data security of CI is an issue. Current practices of data security are to a high degree equivalent to virtual massive data shredding. It is a big obstacle for the development of CI. An architecture of CI allowing a satisfactory level of data security is proposed in chapter 14, together with organizational and legislative preconditions of CI, and an analysis of barriers to CI.

Chapter 16, “Collaborative Practices in Computer-Aided Academic Research,” focuses on sharing information through global communication systems in the context of computer-aided academic research: more specifically, on cross-disciplinary research primarily involving collaborations between natural scientists and colleagues in computational science. The authors’ interest lies in the visualization and high performance computing (HPC) communities, branches of computational science providing enhanced ways of organising, analysing and presenting materials, models and results of research in other disciplines.

In recent times, the focus of innovation is increasingly moving beyond the centralized R&D programs of large firms to more collaborative innovation. This is true even in the Information Communication Technology (ICT) industries. With this approach in mind, the technical strategy has to be laid down to design appropriate architectural models that act as key foundations of building large software systems without compromising access rights, privacy, confidentiality, ethics, policies, IP, etc. A platform that can enable researchers to share their views, ideas, thoughts or products in a seamless manner is needed. Chapter 17, “Designing Appropriate Frameworks, Models, Strategies and Solutions,” examines the ways and means of creating a standard model which focuses on well proven software design practices to leverage the full potential of an open innovation platform while focusing upon the evolution of IP trends and without compromising on access rights, privacy, confidentiality, ethics, policies, IP, etc.
Developments in technology and the global nature of business means that personal information about individuals in the UK may often be processed overseas, frequently without the explicit knowledge or consent of those individuals. This raises issues such as the security of such data, who may have access to it and for what purposes and what rights the individual may have to object. The Data Protection Act 1998 provides a standard of protection for personal data, including in respect of personal data that is being transferred outside of the UK. Chapter 18, “International Transfers of Personal Data: A UK Law Perspective,” focuses on how a UK data controller (the organisation that controls how and why personal data is processed and is therefore legally responsible for compliance) can fulfill its business and operational requirements in transferring personal data outside the EEA, whilst ensuring legal compliance.

In Turkey, access blocking to websites by judicial orders has especially come into spotlight with the blocking of globally renowned websites such as www.youtube.com and www.wordpress.com. After police operations in 2006 that concentrated on Internet child pornography, the need for legal provisions to regulate the Internet has been widely discussed and Law No. 5651 on the Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publications was enacted on May 25, 2007. This law has generally defined the actors related to the Internet and has regulated access blocking in the scheme of suppression of crimes. Telecommunications Communication Presidency is entitled to the enforcement of the law that has come into effect as of October 23, 2007. Chapter 19, “Restricted Access and Blocking Websites, Internet Regulations and Turkey Practices,” aims to trace the short history of access blocking and try to assess the subject in the light of cases from the applications in Turkey.

The third section, “Protection of Privacy and Trust,” includes three chapters concerned with unauthorized accesses to sensible digital information, privacy rights and trust, and presents tools and techniques to prevent or control these aspects.

In chapter 20, “Hardware Secure Access to Servers and Applications,” the authors propose a powerful yet inexpensive method for protecting and discriminating unauthorized accesses to sensible digital information (or even to the entire system) via common and conventional tools such as USB devices. The result of this work is that access to servers or the execution and access to specific data takes place only under a controlled and defined scenario.

According to chapter 21, “Ensuring Users’ Rights to Privacy, Confidence and Reputation in the Online Learning Environment: What Should Instructors Do to Protect Their Students’ Privacy?” there is no clear right to privacy, confidence, and reputation in United States case law or in legislation for students in the online environment. While some privacy interests are protected under a variety of legal theories, none expressly applies to online education. The study presented examines pertinent issues concerning the privacy rights of students while engaged in online learning. A survey of students using online tools in their courses demonstrated a widespread belief that their communications were private. A second survey of business law instructors using online tools revealed a lack of awareness of the potential for abuse by third parties able to access users’ information. Survey results were inconclusive with regard to the existence of policies and procedures within the institutions with regard to protecting users’ privacy rights in online instruction. Survey respondents made several recommendations for action to mediate the lack of existing protections for privacy in online learning.

Passive network monitoring is very useful for the operation, maintenance, control and protection of communication networks, while in certain cases it provides the authorities with the means for law enforcement. Nevertheless, the flip side of monitoring activities is that they are natively surrounded by serious privacy implications and, therefore, they are subject to data protection legislation. Chapter 22,
“Legislation-Aware Privacy Protection in Passive Network Monitoring,” investigates the challenges related to privacy protection in passive network monitoring based on a joint technical and regulatory analysis of the associated issues. After introducing the issue and its special characteristics, the chapter provides background knowledge regarding the corresponding legal and regulatory framework, as well as some related work. It then delves into the description of the legal and regulatory requirements that govern network monitoring systems, before providing an overview of a reference monitoring system, which has been designed with these requirements in mind.

The fourth section, “Access Rights,” discusses both Web accessibility legislation and standards, and legal aspects of access to digital contents and intellectual property rights.

The Council of the European Union is developing some strategies about the European Digital Libraries considered as a common multilingual access point to Europe’s digital cultural heritage. The project introduced in chapter 23, “The Project of the Ancient Spanish Cartography E-Library: Main Targets and Legal Challenges,” concerning a digital cartographic database accessed through GIS, looks for the integration of digital technologies with the cartographic heritage providing new approaches to and new audiences for the history of cartography. The online presence of this cartographic material will be a rich source of raw material to be reused in different sectors and for different purposes and technological developments; but we must also afford some legal challenges because digitisation presupposes making a copy, which can be problematic in view of intellectual property rights (IPR). As the transparency and clarification of the copyright status of works is very relevant to us, those legal challenges and their solutions will be the main subjects of this chapter.

In contrast with centralized or hierarchical certification authorities and directory of names, other solutions are now gaining momentum. Federation of already deployed security systems is considered the key to build global security infrastructures. In this field, trust management systems can play an important role, being based on a totally distributed architecture. The idea of distributed trust management can be confronted with the concept of trusted computing. Though having a confusingly similar denomination, the different interpretation of trust in these systems drives to divergent consequences with respect to system architectures and access policies, but also to law, ethics, and politics. While trusted computing systems assure copyright holders and media producers that the hosting system will respect the access restrictions they defined, trust management systems instead allow users to grant trust to other users or software agents for accessing local resources, as discussed in chapter 24, “Trusted Computing or Distributed Trust Management?”

Web accessibility is a major question in present ICT legislation. An aging population is a known phenomenon that makes older people become a specific interest group. In chapter 25, “Senior Web Accessibility: Laws, Standards and Practices,” the authors present the evolution encountered in laws and standards due to specific concern about older people. This publication is related to the works of the W3C WAI-AGE group. The authors focus mainly on the adaptations encountered in W3C accessibility guidelines (WCAG) while considering the difficulties related to aging. The chapter also proposes some practical recommendations for Web designers that want to develop websites targeting seniors, and finally gives some perspectives about accessibility legislation and standards.

The last section, “ICT Ethics,” include two chapters that discuss legal, privacy and security aspects related to ICT ethics in the information and knowledge society.

Chapter 26, “E-Health at Home: Legal, Privacy and Security Aspects,” describes the present situation of e-health at home, taking into account legal, privacy and security aspects. As a first step, some background and a general description of e-health activities at home are presented. In order to have a
general idea of the current status of this field, we analyze the general legal situation in terms of ICT for E-health and several related issues on data mining privacy and information recovery aspects. The topics covered include the taxonomy for secondary uses of clinical data and a description of the role that controlled vocabularies play. Concerning the provision of e-health at home, the chapter revises the current situation in the digital home evolution including topics on sensors and sanitary devices. Furthermore the challenge of digital identity at home and the differences between the domestic environment and the professional one are considered. Finally, some ethical considerations under the “InfoEthics” concept and future lines of work are addressed.

“Informational Society” is unceasingly discussed by all societies’ quadrants. Nevertheless, in spite of illustrating the most recent progress of western societies the complexity to characterize it is well-known. In such societal evolution, the “leading role” goes to information as a polymorphic phenomenon and a polysemantic concept. Given such claims and the need for a multidimensional approach, the overall amount of information available online has reached an unparalleled level, and consequently search engines become exceptionally important. Mainstream search engine literature has been debating the following perspectives: technology, user level of expertise and confidence, organizational impact, and, just recently, power issues. However, the trade-off between informational fluxes versus control has been disregarded. Chapter 27, “Controlling Informational Society: A Google Error Analysis!” discuss such gaps, and the overall structure of the chapter is: information, search engines, control and its dimensions, and exploiting Google as a case study.

EXPECTATIONS

This book offers an exhaustive coverage on the theme, providing researchers, scholars, and professionals with some of the most advanced research discussions, developments and solutions on the domain of ICT law, protection and access rights in a very comprehensive way.

This book intends to support the academic audience (teachers, researchers and students, mainly of post-graduate studies), law, IT and ICT professionals and managers and policy makers of a broad range of sectors.

We sincerely expect that this work will stimulate further research and development on the theme by law and IT professionals and researchers, academics and doctoral students, policy makers and top managers.

The Editors,

Irene Maria Portela
Polytechnic Institute of Câvado and Ave, Portugal

Maria Manuela Cruz-Cunha
Polytechnic Institute of Câvado and Ave, Portugal