

## Re-using case law across Europe: legal barriers to be faced

MARIA ANGELA BIASIOTTI\*

SOMMARIO: *1. Introduction – 2. The Caselex domain and data process – 3. Caselex legal scenario – 4. Caselex data process workflow – 4.1 Legal barriers in data acquisition – 4.2. Legal barriers in data processing – 4.3. Legal barriers in data access – 5. Conclusions – 6. Appendix: European countries legislation on copyright*

### 1. INTRODUCTION

Caselex is a project financed by the European Commission under the e-Content Program aiming at offering access to case law across European borders facing the difficulties deriving from different legal traditions. Fueled by public funding and through a consortium blending private and public sector parties, CASELEX has created a system offering an Internet based “one-stop-shop” service for important national case law linked to the common denominator of EU law, i.e. decisions of Supreme and High Courts, within selected areas of law connected to the implementation and application of EU law. As such it aims to serve as a European service, accessing and converting the comprehensive base of public case law into easy obtainable and usable knowledge for distribution throughout Europe. For building up Caselex system every strategy and implementation have been chosen according to previous surveys and studies.

Case law is an important source of public sector information (PSI) as output of the judiciary, together with information of governmental bodies, jointly constitute the so-called ‘basic information of the democratic constitutional state’ and it is generally accepted that these categories of PSI should be more and more accessible and available as wide as possible.

The creation of this type of information is by definition a public task and its wide dissemination serves public interests.

\* The Author is a junior researcher at the Institute for Legal Theory and Techniques of the CNR engaged in the study and analysis of “Advanced tools facilitating the knowledge of law at European Union level”. Issues here described have been deeply analysed in a report written by a working group engaged in the development of the Caselex Project (M.A Biasiotti, S. Faro, E. Francesconi, R. Nannucci, L. Serrotti, P. Spinosa and D. Tiscornia).

Caselex has during 2005 and 2006 developed a deep understanding of the key issues surrounding the European service opportunity and associated issues, and in response developed a platform to overcome the practical barriers of establishing an online service that can support and link the vast repository of important case law of national and European courts with European relevance. Facilitating and linking such material, would imply an enormous benefit to the legal community and society at large, in particular practitioners such as courts, law firms and lawyers in need of such knowledge sources in their daily work.

In order to provide added value services related to Case law contents, the Caselex content and knowledge management procedure had to deal with several processes such as acquiring, retrieving, analysing, processing, managing and re-using case law data.

As a result, Caselex had to cope with a very heterogeneous framework which is taken into account in the following analysis and more specifically with technical and legal barriers related to the different sources and the processes involved.

In order to properly discuss and treat legal barriers it is of paramount importance to link their analysis to the description of the overall Caselex process and to identify how content features and semantic and linguistic issues constitute barriers hampering project development.

To perform such an assessment, the data management process followed by the Caselex service platform is here after briefly described. This process can be synthesised according to its interaction both with content holders and end-users. In particular the structure of the Caselex data management process can be represented by three main stages: data acquisition, data processing and data access. Whereas:

*Data acquisition* is the stage describing the process and mechanism for data transfer from local case law content holders to Caselex implying the analysis of the following legal barriers: IPR (Intellectual Property Rights) and Database protection, DRM (Digital Rights Management), Licensing.

*Data processing* is the stage intended to transform information collected into added value services to end-users. In particular this process implies: the conversion of proprietary format data into data in the Caselex format; adding metadata: (to make information retrieval easier for end-users; and to increase the quality of the information provided.

These activities imply the analysis of the following legal issue: DPR (Personal Data Protection Rights) as to parties involved in the decision.

*Data access* is the stage representing the interaction modalities between the Caselex service and end-users. In particular, it takes into account information retrieval and presentation barriers and how to overcome them (e.g. different query languages and heterogeneous devices). This stage implies the analysis of the following issue: DPR as to end-users.

## 2. THE CASELEX DOMAIN AND DATA PROCESS

The Caselex platform service implies the analysis and proper management of a set of specific issues related both to information communication technology and to the legal and judicial domain. Within this perspective some key factors can be identified.

<i>National and EU Legislation</i>	The Caselex platform is required to comply with EU Member States' legislation and EU laws on DPR, IPR, DRM, security and access rights.
<i>Multilingual Aspects</i>	In order to ensure wide acceptance and use of the Caselex service, the platform has to assure the proper management of linguistic issues, in terms of multilingual interface, content, access and data management.
<i>Added Value Information</i>	In order to be effective, the Caselex service will provide end-users with the fulltext of a decision plus "added value" information. The added value information should provide different levels of support to document retrieval, such as summary, proper cross-referencing (hyperlinks), categories based on classification schemes, and other different types of metadata.
<i>Technology</i>	Technology – which greatly influences the overall acceptance of the Caselex service – is an important factor to enhance user-friendliness and data security as well as data management inexpensiveness, rapidity and reliability. Since technology is evolving extremely fast, a specifically-oriented technology might become obsolete in a short time. A scalable and expandable service architecture, based on international and open standards, is therefore recommended.

<i>Interoperability</i>	Interoperability refers to attributes of the software platform that affect its ability to interact with other systems. It makes possible data understanding and exchange among different operators. The use of standards does not on its own ensure interoperability since independent applications may implement different subsets of optional parts of a standard. As a consequence it is very important for Caselex to define different standard solutions for each particular application class (mostly for multi-media devices). Systems are interoperable when they can also execute a common task together, in addition to communicating with each other. This requires additional standards such as APIs (Applications Programme Interface)
<i>Acceptance</i>	In order to be effective, the Caselex initiative needs to be well accepted by all agents involved: public and private institutions and stakeholders. In general, a service is well accepted when it is regularly and at short intervals updated, user-friendly and secure and its content is of high quality

### 3. CASELEX LEGAL SCENARIO

During the first phase of the Project information was collected from different content holders in EU and EFTA Member States in order to carry out a survey of the current state of art relevant to existing services provided in terms of:

- what kind of content is disseminated;
- how information access is regulated;
- how IPR, database protection and DPR are managed.

It resulted that:

- most European countries have not yet transposed the Public Sector Information Directive;
- in about half the countries court decisions are disclosed via a central public organisation, or plans exist to do so, while in the other half disclosure takes place via the courts themselves, or via commercial or semi-commercial organisations;
- most public content holders have no settled standard licence policies;

- in most “old” Member States, (supreme and constitutional) court decisions are available to the public free of charge, while in most “new” Member States only a limited amount of (supreme and constitutional) court decisions are available to the public free. Apart from the few (supreme and constitutional) court cases available free in the new Member States, all the rest are made available by commercial organisations and are not available free of charge;
- half of the public content holders make no distinction between commercial and non-commercial re-use of court decisions;
- most of the public content holders impose conditions of re-use (citation of the court giving the decision and prohibition on amending the decision);
- in most European countries, there is no copyright on case law (on the other hand, added value, in the form of summaries or translations of court decisions, is usually protected by copyright legislation);
- most public content holders hold database rights (copyright and *sui generis*) on their case law databases, but do not exercise them. Many of them are not aware of this protection.

#### 4. CASELEX DATA PROCESS WORKFLOW

##### 4.1. *Legal barriers in data acquisition*

The data acquisition phase describes issues and possible methodologies for accessing and acquiring data provided by different European case law content holders and populating the Caselex repository. Case law management at European level has to cope with the different sources and legal systems of each country. Referring to this scenario, Caselex had to analyse the services provided by each content holder and consequently take pertinent decisions for proposing specific agreements and data acquisition protocols to content holders.

Referring to *legal issues*, the acquisition process implies a specific written agreement between Caselex and each case law content holder in order to guarantee data acquisition and re-use. The agreement should clarify all legal and economic aspects and provide in particular for the proper management of issues such as IPR, Database Protection<sup>1</sup> and Digital Right Management.

<sup>1</sup> For a more detailed description of the scenario see the Annex at the end of this paper.

The following part provides an overview of the most relevant legal issues related to the acquisition and re-use of case law, regarding, specifically, intellectual property rights – in particular, copyright –, database protection, digital right management and licensing .

#### 4.1.1. Intellectual property rights: copyright

The analysis of this issue can be done distinguishing between copyright on decisions and copyright on added value information.

As to Copyright on decisions<sup>2</sup> Article 2 (4) of the Berne Convention on Copyright states: “It shall be a matter for legislation in the countries of the Union to determine the protection to be granted to official texts of a legislative, administrative and legal nature, and to official translations of such texts.” This means that Copyrights are not absolute rights and most countries in the world recognise the need to limit the exclusive rights given to authors in certain specific circumstances. These limitations and exceptions ensure that access to information to further the public interest in research, education and other important policy goals is not subject to unnecessary copyright restrictions.

According to the Berne Convention (all EU and EFTA countries are party to the convention), there is no copyright on case law in most European countries. On the other hand, where copyright is provided for, rights belonging to public institutions are usually not exercised: this means that normally the full-text of decisions can be used without any constraints.

In all likelihood this situation could change in the future with the implementation in EU Member States of Directive 2003/98/EC on the Re-use of Public Sector Information. This Directive concerns all generally available documents held by public institutions (concerning not only the political process but also the legal and administrative process); but the nature and relevance of the changes will depend on the specific national implementation measures, as the Directive “does not contain an obligation to allow re-use of documents. The decision whether or not to authorise re-use will remain with the Member States or the pub-

<sup>2</sup> Council of Europe, “European Convention for the Protection of Human Rights and Fundamental Freedoms”, <http://conventions.coe.int/treaty/en/Treaties/Html/005.htm>.

lic sector body concerned. This Directive should apply to documents that are made accessible for re-use when public sector bodies license, sell, disseminate, exchange or give out information” (see recital no. 9 Directive 2003/98)<sup>3</sup>.

As to Copyright on added value, this type of information (metadata, e.g. summary, classification, translation, etc.) to raw decision text in most cases implies proper management of IPR. If an indexer uses skill and expertise to apply metadata elements to a document, then metadata are protected by copyright.

Copyright is limited only to added information and is generally exercised. Even if copyright is not exercised, metadata can be protected by database rights.

If the value is added by a public institution, whether this copyright is asserted depends on national law; if this is the case, Caselex will require a license.

#### 4.1.2. Database protection

European Council Directive No. 96/9/EC<sup>4</sup> on Legal Protection of Databases provides for the protection of databases. The selection or the database content arrangement is usually protected by copyright. The protection of the investment in creating a database is protected by a *sui generis* right. A database is defined in the Directive as: “*a collection of independent works, data, or materials arranged in a systematic or methodical way and individually accessible by electronic or other means*”

Databases may include any type of information, such as text, sound, images, numbers, facts, or data. Electronic and print databases are covered by the Directive. Catalogues, such as library catalogues, are databases under this definition, as are collections of metadata. The protection granted to databases depends on whether an intellectual or creative effort has been applied to their creation.

<sup>3</sup> For the implementation status of Directive 2003/98/EC see: [http://europa.eu.int/information\\_society/policy/psi/implementation/status/index\\_en.htm](http://europa.eu.int/information_society/policy/psi/implementation/status/index_en.htm).

<sup>4</sup> Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31996L0009&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31996L0009&model=guichett).

Database makers can prevent unauthorised copying for 15 years from the date of completion of the database or from when it was made available to the public. Substantial changes to the database will cause a new 15-year period to run. It is left to Member States to provide for exceptions to this right, such as exceptions for teaching or non-commercial research, etc. According to these provisions, the compilation of court cases, especially if enriched by a collection of original metadata, will give the producer a database right, allowing it to prevent others from copying (substantial parts of) the database.

Also in this case, when the database is created by a public institution, it depends on national law whether this database right is asserted; if the right is exercised, Caselex will require a license.

In order to describe at European level the status related to case law IPR and case law database protection, a specific analysis for each country was performed and its results are reported hereafter attached table:

From the previous survey, the general conclusion is that there is no copyright on case law and, in the few cases where it is foreseen, rights are not actually exercised by public content holders (Germany, United Kingdom, Ireland, etc.).

As to the protection of case law compilation by database rights, the protection by law applicable to databases is in general also extended according to European rules existing within this framework; only in a few cases is decision compilation not protected by such rights.

In conclusion, the IPR issue on raw case law documents does not seem to be a relevant problem, but added value information and database protection represent a crucial issue.

#### 4.1.3. Digital right management

In order to properly manage content and related IPRs, it is important to investigate the DRM issue.

*“The Digital Rights Management is an umbrella term for any of several technical arrangements which empower a vendor of content in electronic form to control how the material can be used on any electronic device with such measures installed”*<sup>5</sup>.

<sup>5</sup> N.F. JOHNSON, J. SUSHIL, *Exploring Steganography: Seeing the Unseen*, 1998, <http://www.jjtc.com/pub/r2026.pdf>.

The main features to be guaranteed are to provide authors, publishers and distributors of digital works with tampering-resistant mechanisms for identifying and tattooing copyrighted materials and monitoring access to and usage of these materials. The proper access and usage management of contents covered by copyright facilitates the royalties accounting.

Several solutions allow the originator of digital copyrighted material to specify appropriate licensing conditions. So, it tightly links these legal technical conditions of use (for example, which actors are allowed to copy or to print) with the material itself. This seamless link persists even if the material is transmitted, sub-licensed or inserted into other digital material; the material is useless if the attached links cannot be deployed properly.

These functions keep records of access and operations by users as well as of detected attempts at illicit usage. These data are used for billing users when usage is to be paid for, and for tracking transactions which take place on the protected material.

In particular, a DRM system may incorporate and make use of technologies such as Self Protecting Documents, Digital Watermarks and Steganography.

A self-protecting document (SPD) contains an encrypted document as well as a secure set of permissions and the software necessary to process the document; full decryption of the document is performed as late as possible so as to minimise the possibility of intercepting the document before it has been fully rendered on screen or paper.

This system reduces the likelihood of unauthorised reproduction and redistribution by either authorised or unauthorised recipients.

Digital watermarks prove ownership and provenance of the images, but cannot stop them being downloaded. They can be visible, partially visible or invisible. Visible watermarks are easier and cheaper to implement, but also tend to spoil the look of the image, so are not ideal for works of art etc. However they do eliminate the commercial value of a copy without preventing its legitimate use. Invisible watermarks are less of a deterrent to illegal use but increase the likelihood of proving that an image has been stolen. More advanced invisible watermarking systems will place the mark on the image at the time of access by the user. Further information can then be added to the mark such as the name and contact details of the user, time of downloading, and agreed copyright terms etc. Similar techniques can be used on audio and video media.

Literally “covered writing”, steganography in the digital area involves hiding information inside something else, usually an image but it could be any digital format such as a piece of recorded sound. Two files are required, the cover image which will hold the hidden data, and the data to be hidden. The two files combine to make a stegoimage which requires a key to decode it<sup>6</sup>.

Furthermore DRM can be managed according to user level authorisation or licensing provided through Automated Payment Systems which implies that if a provider sells services on the Internet, by telephone or mobile device, a secure system able to protect the details of a customer’s credit card is to be considered essential. This will involve a Payment Gateway communicating with the customer’s bank.

It is worthwhile pointing out that the DRM issue has to be faced by Caselex both at the acquisition and at the data access phase.

In fact, digital rights inherited from collected contents should be transferred in full to material distributed by Caselex, so as to guarantee copyright protection, as it is applied to the acquired documents. The processing steps should also keep DRM techniques and methodologies unaltered.

#### 4.1.4. Remarks on legal issues: licensing

The Caselex service, according to IPR and database protection, should respect the legal issues implied. In particular, starting from existing regulations it has to guarantee obedience to such regulations along all the Caselex service provision. Such level of guarantee will also be achieved through specific DRM protocol and solutions embedded in Caselex.

Agreements with content holders will define how Caselex will manage contents and all related legal issues.

It is recommended to pursue a common reference agreement to harmonise relationship and contractual terms with different providers, even if each agreement might require specific customisation according to national laws.

Access to and use of electronic information is usually governed by a contractual agreement, otherwise known as a licence, which is binding upon

<sup>6</sup> [http://en.wikipedia.org/wiki/Digital\\_Rights\\_Management](http://en.wikipedia.org/wiki/Digital_Rights_Management).

both parties. This has become the preferred business method used by copyright owners to regulate content in digital form. A licence does not confer ownership rights; it merely specifies the conditions under which databases and other copyright works can be used and exploited, and by whom.

The EU Copyright Directive 2001/29/EC encourages the use of licences. In recital it says: “*The rights referred to in this Directive may be transferred, assigned or subject to the granting of contractual licences, without prejudice to the relevant national legislation on copyright and related rights*”<sup>7</sup>. This last point is important: licences should not override copyright law.

Licences set out who is entitled to access the work, at what price and on which terms. These terms address questions such as whether a user is entitled to make any copies of the work, for how long a user is entitled to access the work, or whether he can make any changes to it.

In particular, the Caselex Consortium could take on the management of two main licensing typologies, according to licensing policies and regulations applied in each country.

- Standard Licence
- Non Standard Licence

The *Standard Licence* structure could be based on the following elements:

- the Material Covered by the Licence
- how the Material may be Reproduced
- obligations
- changes to the Terms of the Licence
- assignment
- disclaimer

The *Non Standard Licence* could be the result of the following terms:

A	Terms similar to all European States (general part)
B	Terms similar to a group of countries that have the same set of rules
C	Specific terms that are the result of a direct negotiation between Caselex and the content holder

<sup>7</sup> Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEX numdoc&lg=EN&numdoc=32001L0029&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEX numdoc&lg=EN&numdoc=32001L0029&model=guichett).

The economic aspect related to the agreement between Caselex and the content holder will be related to the quality of data provided (added value or raw data) and to the typology of agreement (more or less demanding for the provider).

#### *4.2. Legal barriers in data processing*

Referring to the data processing phase, the most relevant technical element in terms of legal implications is the issue of personal data protection rights related to the parties in a case.

The issue of DPR related to end-users, involving privacy policies and data log management, will be discussed in the Data Access paragraph.

##### 4.2.1. Personal data protection rights (parties involved)

Caselex has to implement a specific procedure to process and disseminate content complying with personal data protection rights<sup>8</sup>.

To cope with this aspect, as it arises from EC directives and national legislation, Caselex has to deal with two main aspects:

- the regulations of the country where data come from, including anonymisation aspects;
- the regulations of the country where the Caselex repository will be located.

In particular the Caselex service has to take into account the fact that:

- every country manages this issue according to its own legal system, anonymising the decisions or not;
- DPR in some countries concerns only natural persons while in other countries it also concerns legal entities;
- in some countries anonymisation is compulsory, in other countries it is performed only at a party's request, in others it is not possible.

As can be seen ahead the situation in Europe is very heterogeneous.

According to the Norwegian Act relating to the Courts of justice, Article 130 (Domstolsloven § 130), courts may anonymise parts or all of

<sup>8</sup> Europa Data Protection Legislative Documents, [http://europa.eu.int/comm/internal\\_market/privacy/law\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/law_en.htm); OECD Privacy Statement Generator [http://www.oecd.org/document/39/0,2340,en\\_2649\\_34255\\_28863271\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/39/0,2340,en_2649_34255_28863271_1_1_1_1,00.html).

a decision if it is in breach of the law on privacy or if it could jeopardise an investigation. (Lovdata, the leading Norwegian content/information provider of statutes, court decisions etc. generally anonymise all parties in criminal cases before they publicise decisions).

In Italy, according to the Code on personal data protection, decisions concerning anonymisation (regarding both natural and legal persons) are taken by the Court (autonomously or at the request of the party).

In Switzerland, when deciding on the way in which the decision is to be published, the president of each court must consider personal data protection legislation.

In France there is a Recommendation of the CNIL (Commission Nationale Informatique et Libertés) concerning the anonymisation of case law diffused freely on the Internet. This recommendation of 29 November 2001 is not a directive, so the debate in France is still open.

As a consequence:

- Caselex will collect anonymous and non anonymous decisions, according to the legislation of the country they come from and, where necessary, to the party's wish; any change of national data protection legislation is irrelevant for data already collected by Caselex (so if Country A enacts legislation providing anonymisation of decisions, this rule will be relevant for Caselex only for decisions collected after the law enters into force);

- the obligation to anonymize decisions depends on the State legislation where data are published, that is of the country where the Caselex Website will be located;

- Caselex could publish all decisions in anonymised form and could then set up its site in any country, whilst taking care to respect any DPR.

However it must be borne in mind that:

- in common law countries decisions (judgements) are generally identified through the parties' name;

- the anonymisation of a decision is not a simple process as it does not mean only eliminating names, surnames or company names, but also cancelling any reference that could identify in an indirect way the party involved (e.g. "the defendant, owner of Microsoft, ...");

- a good example of a software prototype to help anonymisation is the NOME program developed by the University of Montreal, Canada.

Such software is not fully autonomous as it requires considerable human assistance<sup>9</sup>.

In conclusion, if the Caselex site is located in a country where anonymity is not compulsory, it is possible to publish decisions in the same form in which they are acquired.

In such a framework it is fundamental to mention that DPR is a highly regulated issue at European level. In particular, the EU privacy protection model is the foundation of many privacy systems, representing a widely accepted international standard.

The 1995 EU Directive imposes an obligation on Member States to ensure that personal information relating to European citizens has the same level of protection when it is exported to, and processed in, countries outside the EU.

Directive 95/46/EC Art 4 directly addresses this essential question, and reads as follows:

1) National law applicable.

Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

<sup>9</sup> F. PELLETIER ET AL., *L'assistant d'anonymisation NOME*, [http://www.iro.umontreal.ca/~plamondl/docs/Pelletier\\_Paris2004\\_NOME.pdf](http://www.iro.umontreal.ca/~plamondl/docs/Pelletier_Paris2004_NOME.pdf).

2) In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

Referring to European Directive 95/46/EC, it is important to highlight the elements that are relevant for the development of the Caselex service.

The *controller* is defined in Art 2(d) as “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data”.

The definition is neutral as regards the point of establishment of the controller. It is comprehensive as all processing must be attributable to one or more controllers.

The Directive establishes some relevant points:

- for any activity involving personal data processing a controller must be nominated;
- the controller must guarantee observance of the national law of the Member State where this processing is physically performed;
- if processing is divided into several phases carried out in different Member States, the law of the State in which each phase is physically performed must be applied.

However, although each Member State applies its legislation, the intention of the Directive’s drafters is to harmonise data protection laws to increase the development of the internal market so as to promote the free circulation of goods and services.

From the previous analysis, proper DPR management is based on a suitable choice of the places where processing activities are located; in other terms, in which country the Caselex repository will be set up and in which countries data processing will be carried out. Obviously, the simplest choice would be establishing the controller in a single State, grouping repository and processing and using a centralised procedure (accessible via Web) through which the various national correspondents could do their work.

#### *4.3. Legal barriers in data access*

The Caselex Data Access phase is represented by the interaction modalities between the Caselex service and the end-users.

Such interaction is bi-directional and based on the following information flow:

- the end-user sends a request to the Caselex service;
- Caselex provides the end-user with an added value service according to the end-user's request.

Several issues related to personal data protection rights and IPRs are common to different Caselex data process stages. In the implementation of Web interfaces for data access, it will be fundamental to provide specific statements and disclaimers regarding the above issues and the implemented policies.

#### 4.3.1. Personal data protection rights (end-users)

Caselex will be in the position to collect and manage personal data about its users mainly according to two different modalities:

- firstly, when the user voluntarily and consciously supplies data (for example filling in the Caselex subscription form);
- secondly, when data are collected, without user acquaintance, in invisible ways (this happens through an invisible and automatic processing of personal data). Relevant examples of this second modality are represented by Web server logs and cookies.

Web server logs are able to track information and in this way help the administrator to manage the site and analyse its usage. Examples of information that can be tracked include:

- user's Internet protocol address;
- user's kind of browser or computer;
- the number of links clicked within the site by the users;
- the State or country from which the user accessed the site;
- the date and time of the user's visit;
- the name of the user's Internet service provider;
- the pages the user visited on the site.

Cookies, on the other hand, are small bits of text that a server places into a file on the end-user computer's hard drive. Caselex Website could use cookies in order to simplify login procedures, as cookies make it possible to save a user's preferences and login information, and provide personalised functionality. A user will be able to reject cookies by changing browser settings, but this setting will probably disable some of the functionalities of the Caselex Website.

In both cases - data provided by the user and invisible and automatic processing of personal data - Caselex must adopt an appropriate policy for managing data mainly based on principles of confidentiality and security, according to the EU legislation relevant in this field, represented by:

- *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data; and*
- *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.*

As regards European law, three main aspects have to be considered:

1) The controller must process data according to eight general principles:

- fairly and lawfully;
- for limited purposes;
- data must be adequate, relevant and not excessive;
- data must be accurate;
- data must not be kept for longer than is necessary;
- data must be processed in line with the data subject's rights;
- data must be kept secure;
- data must not be transferred to countries without adequate protection.

2) Traffic data, as Web server logs, have to be processed according to provisions under Article 6 Directive 2002/58.

- Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

- Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

- For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility

to withdraw their consent for the processing of traffic data at any time.

- The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

3) Using cookies and similar devices is allowed only for legitimate purposes, with the knowledge of the users concerned (Article 5, par. 3, Directive 2002/58).

Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, *inter alia* about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

The Caselex service should guarantee full transparency and openness about any personal data that is being collected, and about the use of them. It is advisable therefore to have a privacy statement which sets out:

- why Caselex is collecting this personal information;
- what Caselex intends to do with the collected information;
- what options users have when Caselex makes use of their data;
- an explanation of who may have access the data;
- how long Caselex intends to hold data on its system(s);
- whether Caselex uses cookies to track user activity;
- whether Caselex processes data for statistical purposes.

At any point where personal data are collected, people must be allowed to access and consult the privacy statement. The OECD (Organisation for Economic Co-operation and Development) has a privacy policy generator tool which can help anyone drafting a privacy statement. There are numerous examples of privacy statements on the *www*, including, for example, Europe Direct, the University of Leicester and Russian Archives Online.

All requests by data subjects wishing to access their personal details

should be dealt with promptly; and any personal information relating to a third party individual should not be disclosed without the consent of the third party.

## 5. CONCLUSIONS

The present contribution analysed legal barriers that have to be overcome to build a highly qualified Caselex service.

In particular, they have been assessed, specifying them within the three identified Caselex data management process phases (Data Acquisition, Data Processing and Data Access).

Most of the issues discussed typically appear during the creation of a Web service providing multilingual documentation collected by different content holders, stored in a unique repository and addressed to a variety of user categories speaking different languages.

All specific aspects related to the analysed information (court decisions) and to end-user needs, considering them as expert professionals asking for advanced tools to recover information have been analyzed.

In conclusion, a scenario emerges where:

- each legal barrier can be overcome through a variety of solutions. Generally speaking, each solution derives from the utilisation of different technologies, which also implies a large and differentiated range of costs as to software to be developed, human resources to be employed (during the experimentation and afterwards) and the time to be applied to each decision;

- each solution adopted has an impact on the quality and quantity of both data and applied metadata but also on retrieval possibilities.

A satisfactory balance between costs and expected results, which may however guarantee high quality data and proposed Caselex service functions, is greatly recommended. This criterion should be applied especially in those cases in which the Report has suggested a variety of possible solutions to be assessed in light of Caselex requirements and feasibility.

Once strategic choices are properly made, the creation of a highly qualified service as required by potential Caselex users may become an available and a real possibility.

## 6. APPENDIX: EUROPEAN COUNTRIES LEGISLATION ON COPYRIGHT

<b>Belgium (BE)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Law applicable: Law on copyright and neighboring rights of June 30, 1994 modified by the law of April 3, 1995 and the law of August 31, 1998. The law of August 31, 1998 implementing the European directive of March 11, 1996 on the legal protection of databases is also applicable. And so is the law of June 30, 1994 implementing the European directive of May 14, 1991 on the legal protection of the software	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15762&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15762&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	
<b>Switzerland (CH)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Law applicable: Federal Act on Copyright and related rights of October 9, 1992 (Articles 4 and 5)	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15353&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15353&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	
<b>Czech Republic (CZ)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Law applicable: Copyright Act n°121/2000 of April 7, 2000	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15324&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15324&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	
<b>Germany (DE)</b>	
Copyright on case law: Yes (not exercised)	Protection of compilation of case law by database rights: Yes (not exercised)
Law applicable: Gesetz über Urheberrechte und verwandte Schutzrechte (Urheberrechtsgesetz) which came into force on January 1, 1966	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=22403&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=22403&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	
<b>Denmark (DK)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Act on copyright - Consolidated act no. 164 of march 12, 2003	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=22368&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=22368&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Estonia (EE)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Law of November 11, 1992 modified the 18th of November 2002 (Article §5.4 (1) and article §4.3) [Exceptionally, the translations of judgements are subject to copyright, but this right has never been exercised] Act on copyright - Consolidated act no. 164 of march 12, 2003	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15287&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15287&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Spain (ES)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Intellectual Property law of June 12, 1996	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15285&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15285&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Finland (FI)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: No
Copyright Act (Tekijänoikeuslaki): law n°404 of July 8, 1961 amended in 1998	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15340&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15340&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>France (FR)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Intellectual Property Code 1994 (Loi 2003-706 du 01/08/03), modified in 2003 (art. L. 341-1)	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15288&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15288&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Greece (GR)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Law 2121/1993, amended by the law 3057/2002 implementing the European dir. 2001/29	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15343&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15343&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Hungary (HU)</b>	
Copyright on case law: Yes	Protection of compilation of case law by database rights: No
Information Law n°LXXVI of 1999 on Copyright	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15295&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15295&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Iceland (IC)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Copyright Act 73/1972 with later amendments	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15345&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15345&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Ireland (IE)</b>	
Copyright on case law: Yes (not exercised)	Protection of compilation of case law by database rights: Yes (not exercised)
Copyright and Related rights Act, 2000	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15313&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15313&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Italy (IT)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Copyright Law n°633 of 1941, last modified in 2003. (Articles 5 and 102 bis seq.)	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=27690&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=27690&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Liechtenstein (LI)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Law of May 19, 1999 regarding Copyright and neighboring rights	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15347&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15347&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Lithuania (LT)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Law amending the law on copyright and related rights of March 5, 2003	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15314&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15314&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Latvia (LV)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Copyright law of April 6, 2000	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=18620&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=18620&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Malta (MT)</b>	
Copyright on case law: Yes	Protection of compilation of case law by database rights: Yes
Copyright Act XIII of 2000, as amended by Act VI of 2001	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15318&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15318&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>The Netherlands (NL)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: No
Law on Copyright of September 23, 1912, amended by the law of March 6, 2003 Law on neighboring rights of March 18, 1993 amended by the law of March 6, 2003 Law on databases of July 8, 1999	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15350&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15350&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Norway (NO)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: No
Act n°2 of May 12, 1961 relating to copyright in literary, scientific and artistic works, etc. amended the 1st of July 2001 (Article 43)	
Web: <a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15319&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15319&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Portugal (PT)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes
Decree law of March 14, 1985 no. 63, as amended by the law of Aug. 2001 (Art. 7 and 3) Law Decree 122/2000, of 4th July (sui generis right on databases)	
<a href="http://portal.unesco.org/culture/en/ev.php-URL_ID=15320&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html">http://portal.unesco.org/culture/en/ev.php-URL_ID=15320&amp;URL_DO=DO_TOPIC&amp;URL_SECTION=201.html</a>	

<b>Sweden (SE)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: No
Swedish Act on Copyright in Literary and Artistic Works (article 9, 26 and 49) March 1, 1996	
Web: <a href="http://www.kb.se/BIBSAM/KJELL/urleng.htm">http://www.kb.se/BIBSAM/KJELL/urleng.htm</a>	

<b>Slovenia (SI)</b>	
Copyright on case law: No	Protection of compilation of case law by database rights: Yes

Copyright and Related Rights Act of 30 march 1995 as amended on 26 january 2001, 10 april 2001, and on 9 april 2004 (as in force from 11 may 2004)

Web: [http://portal.unesco.org/culture/en/ev.php-URL\\_ID=17095&URL\\_DO=DO\\_TOPIC&URL\\_SECTION=201.html](http://portal.unesco.org/culture/en/ev.php-URL_ID=17095&URL_DO=DO_TOPIC&URL_SECTION=201.html)

### **United Kingdom (UK)**

Copyright on case law: Yes (not exercised)	Protection of compilation of case law by database rights: Yes (not exercised)
---	--

Copyright, Designs and Patent Act 1988

Web: [http://www.opsi.gov.uk/acts/acts1988/Ukpga\\_19880048\\_en\\_1.htm](http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm)