



The Legal PACER



No. 3

The legal Newsletter of  for the PACE project

Winter 2001

E-Content Programme adopted by the European Council

The European Council has adopted on 22 December 2000 a new four year programme called *eContent*. This programme aims at supporting the production, the dissemination and the use of European digital content and at promoting a linguistic diversity on the global networks. This programme is part of the *eEurope* Action Plan focusing on the great possibilities provided by the digital technologies across Europe.

The main concern of this new programme is the access and the use of the public sector information taking into account the expansion of the information supply and the linguistic and cultural adaptation of information products.

The second action line of this programme will be devoted to "Demonstrating exploitation of public sector information".

In that framework, questions interesting PAs will be developed. For example, *the e-CT* project will analyse the possible public-private partnerships in order to facilitate access to and use of Public Works calls for tenders. The *PSINET* project will explore the potential of Europe's Public Sector Information resources in digital Content products and services through cross-border as well as public private partnerships.

More information on the events and progress of the *eContent* programme : <http://www.cordis.lu/econtent/>

The huge cost of "junk" e-mails

A study undertaken by the European Commission reveals that Internet users world-wide spend an extra Euro 10 billion a year in connection costs to receive the so called "junk" e-mails. The purpose of the study is to highlight the importance of privacy and data protection in the daily use of the Internet and more specifically in the development of e-commerce. Focus is put on the different approaches existing within the EU members in the process of implementing the directive on data protection in their national law.

It is indeed noticeable that EU member states pursue different ways to implement the concepts enshrined in the directive for the protection against "junk" e-mail or "spamming".

Protection can be provided by the *opt-out technique*, which consists in expressing the wish not to receive such unsolicited messages. Countries such as Austria, Denmark, Finland, Italy and Germany are applying the *opt-in technique* for which a formal request to receive the message is requested.

For more information on the study:

http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/spam.htm

Calls for Tenders Databases

Since last year, many web sites devoted to call for tenders publicity have been developing databases allowing businesses to proceed detailed searches of contract notices:

- **Belgium** : <http://www.webshapes.be/ebp/>

This is a Belgian consulting company that provides information related to calls for tenders according to clients requests.

- **Germany**: <http://www.medienpool.com/>

Medien Pool is a databank system that facilitates a safe, fast and easy online exchange of the invitation of tenders documents between customer and order taker.

- **France**:

<http://www.journal-officiel.gouv.fr/boamp/r1.htm>

French calls for tenders handled by *The Journal Officiel*.

In France, the government is currently launching a pilot website, SAOMAP, which ultimate aim is to add to the database the possibility of downloading all the technical documents related to Public Works calls for tenders.

<http://saomap-sctb.fr>

- **Italy**: <http://www.informatel.it/>

This website contains a database of calls for tenders.

- **Ireland**: <http://epin1.epin.ie/EPINIE.htm>

EPIN is a business development tool which provides companies with access to a database of contract notices.

- **UK** : <http://www.tenders.co.uk/>

"Tenders on the Web" is a fully searchable database of European public procurement contracts.

War to cybercriminals

The English government has created a new "cyberpolice" against paedophiles, spammers and all kinds of computer hackers.

The aim of this new institution is to give confidence in e-commerce. As a matter of fact, recent studies have proved that the lack of investments in e-commerce is due to the lack of confidence in the technical level of installations. Banking on line, for instance, is impeded by the insecurity of the technical installations. One will remember the misadventure of Egg, the first English Bank to be 100% on-line, which was hacked last summer.

This initiative is included in the "Crime Reduction" government programme launched in 1999, which aim is to reassure the population about the insecurity climate on-line and off-line.

E. Wery, [http://www.droit-](http://www.droit-technologie.org/fr/1_2.asp?actu_id=-1429735365)

[technologie.org/fr/1_2.asp?actu_id=-1429735365](http://www.droit-technologie.org/fr/1_2.asp?actu_id=-1429735365)



This Newsletter is published by the Centre de Recherches Informatique et Droit (CRID) from the University of Namur (FUNDP), Belgium, for the IST project PACE.

Contact: Prof. Y. Pouillet

Ms. G. de Villenfagne (geraldine.devillenfagne@fundp.ac.be)



Public Administration and e-Commerce in Europe

Computer Crime

New Belgian legislation of 28/11/2001

Belgium published on 3 February 2001 its new law on Computer Crime. (http://www.moniteur.be/html_fr/bsf00.htm)

International legal bases

First of all, the works of the O.E.C.D. inspired the Belgian legislator (see O.E.C.D, *Guidelines for the security of information systems*, 1992, OECD/GD (92) 190, available on http://www.oecd.org/dsti/sti/it/secur/prod/e_secur.htm).

Secondly, the Belgian legislator based his work on two recommendations adopted by the Council of Europe in 1989 and 1995. The first one is about criminality in relation with computer and the latest one treats specifically procedural questions (see <http://cm.coe.int/ta/rec/1989/89r9.htm> and <http://cm.coe.int/ta/rec/1995/95r9.htm>).

The Council of Europe published also a draft convention on Cyber-Crime which inspired largely the Belgian legislator. Draft N°25 REV., 12/22/ 2000 available on <http://conventions.coe.int/treaty/EN/projets/cybercrime25.htm>

Belgian law

The first part of the law introduces essentially four new computer-related offences in the Criminal Code while the second part clarifies the procedural aspects related to networks and systems.

The four new offences are: computer-related forgery, computer-related fraud and the offences against the confidentiality, integrity and availability of computer data and systems: hacking and computer sabotage. A simple attempt of all these actions as well as aiding or abetting are sanctioned. The corporate liability is recognised.

The procedural aspects of the law extend the judge's power and permit to go across the frontiers to copy computer data if necessary. Such a permission is not given by the draft convention of the Council of Europe.

Other computer crime legislation

Stein Schjolberg, the Chief Judge of the Moss Byrett Court in Norway, has compiled a collection of International legislation dealing with computer crime. Its website lists the 37 countries that have penal legislation dealing with the "unauthorized access" of computers and computer systems.

See: <http://www.mossbyrett.of.no/info/legal.html>

E-identity

Belgium intends to replace the identity card of its citizens by an electronic identity card. This project follows the line of the modernisation of the Public Administrations (PAs) and is the visible part of the process of rising PAs on-line. This new card could also integrate other functionalities which are still to be studied.

Frank Robben, responsible of the "Federal Information and Communication Technologies Department" (Fedict) affirms that this unique card could also integrate the driving licence and the Belgian medical care card called SIS card.

In this context, Mr Robben explains that the e-card is an identification means coupled with an authentication means (the carrier of the card proves that he is the titular of the identity indicated on the card). It could also become a tool to carry data or programs as well as a smart device to gain access to a specific place (e.g. library). Moreover, it could be a practical means of payment, like an electronic purse.

Frank Robben is not in favour of adding too much data on the card because he considers that the operations of registering and changing data are too delicate. He suggests that the card constitutes an access key to information staying on a network.

Of course the security is a crucial issue in this new system. The exchanges of data between the PAs themselves and their clients (citizens and firms) have to be protected.

The Public Key Infrastructure would be chosen to ensure this. When the card of a citizen will be registered, in the meantime, the citizen will have the possibility to link a private key to his card. This private key saved on another chip-pin card, protected by a personal code, would allow the citizen to use his electronic signature, legally recognised, vis-à-vis the Public Administration.

However, the e-identity card will be more than a simple "memory card". It will be a microprocessor-equipped card, comparable to a computer, executing programs.

If everything turns right, the "e-identity card" will appear in May 2003. Such a project raises serious concerns for privacy as such an e-identity card sounds like a perfect tool for Big Brother purposes...

The first example of an electronic ID card to facilitate on-line transactions with various governmental authorities was introduced in Finland in December 1999. The ID card, which can be obtained by application to the Finnish police, is already held by over 6,000 Finns.

For more information:

<http://www.Lalibre.be>, 08/02/2001(FR)

http://www.tt.fi/arkisto/gethtml.pl?ft_cid=1114(EN)

<http://www.fineid.fi/default.asp?path=1%2CGeneral&file=4%2C>

Visit Crid's website:



<http://www.droit.fundp.ac.be/crid>

Visit the PACE website:

<http://www.pace-eu.net>



Public Administration and e-Commerce in Europe