‘’Personal financial data: Regulatory framework of their e-processing focusing on the function of interbanking information systems in Greece and France’’

By

Milossi Maria

Attorney -at - Law, DESS

PhD candidate in Computer Law, Department of Applied Informatics, University of Macedonia

mariamilossi@yahoo.gr

&

Dr Alexandropoulou –Egyptiadou Evgenia

Associate Professor in Computer Law, Department of Applied Informatics, University of Macedonia

ealex@uom.gr

Keywords: personal financial data, processing, regulatory framework

1. Introduction

This study aims to present the Greek and French legal framework in force about the electronic processing and the legal protection of one of the most significant categories of personal data, the personal financial data. Especially in this study will be presented apart from the European Directives, the national laws as well as the decisions of National Data Protection Authorities (www.dpa.gr and www.cnil.fr).

.

2. Personal financial data: Their meaning and their content

With the term personal financial data or personal data of individual's economic behaviour, we mean the data which refers to the individual's economic situation. It concerns his property, bank accounts, financial transactions, etc.

The personal financial data run through an important part of the individual's day living, as far as almost all the fields of his social life contain personal financial information, either he goes physically to the shops or he uses the benefits of information technology, (by paying with his credit card, or by logging in a website with his ID and password). That means that he has the possibility without moving from his house or his work place, to pay with electronic money, to buy and sell goods and services via internet, to participate in auction sites (e-commerce), to use web banking services (e-banking), to make a flight reservation and pay his e-ticket (e-transport), to buy a concert ticket by choosing his seat (e-entertainment), to submit digitally his tax statement (e-government).

The importance of studying the legal aspect of the individual's personal financial data lies to the fact that these are often a necessary tool for those who deal or aim to deal with this person, in order to be informed about his credit status and thus estimate the relative insolvency risks. All the enterprises and mostly the banks, categorize their clients according to their transactions and their consuming habits. That is because "la valeur du client est l'intérêt du client aux yeux de l'entreprise'' (Girot,2005). Thus, by creating their client's economic profile, the enterprises can plan their commercial actions.

3. Privacy and processing of financial personal data

Apart from the benefits that a web transaction offers to the data subject (that is mainly the considerable saving of money and time), this procession hides many dangers for his privacy. That happens because every single click on the web, leaves its traces on the cyber space. When a transaction takes place on the web, the company that accepts the individual's personal data has the chance to create his personal economic profile and formulate its opinion about his economic situation, his tax status as well as his consuming habits (Chatillon, 2007). These traces on the web language are called 'cookies', that is a text string stored by a user's web browser, consisting of one or more name-value pairs, containing bits of information, which may be encrypted for

information privacy and data security purposes. The cookie is sent as an HTTP header by a web server to a web browser and then sent back unchanged by the browser each time it accesses that server. A cookie can be used for authentication, session tracking (state maintenance), storing site preferences, shopping card contents, the identifier for a server-based session, or anything else that can be accomplished through storing textual data. Cookies' usage enables the fast information flow and reduces the time needed for the user to reenter to the same web page. However, this procedure enables the suppliers to organize the web visitors' data, in order to treat them and then exploit them for commercial purposes, some times without the consent of the interested person.

For the accomplishment of the said purposes, different mathematical methods (Igglezakis, 2003) are being used from the companies such as: a. Credit scoring: It is one of the most successful applications of statistical and operations research modeling in finance and banking. It is the set of decision models and their underlying techniques that aid lenders in the granting of consumer credit. These techniques decide who will get credit, how much credit they should get and what operation strategies will enhance the profitability of the borrowers to the lenders. b. Data Warehouse: A data warehouse is a repository of an organization's electronically stored data. Data warehouses are designed to facilitate reporting and analysis. The means to retrieve and analyze data, to extract, transform and load data, and to manage the data dictionary are also considered essential components of a data warehousing system and c.Data mining**:** It refers to the process of extracting patterns from data. Data mining is becoming an increasingly important tool to transform this data into information. It is commonly used in a wide range of profiling practices, such as marketing, surveillance, fraud detection and scientific discovery.

One of the results of all these methods is the spamming, that is defined as the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media (junk fax transmissions, social networking spam, television advertising and file sharing network spam, etc). Spamming is universally criticized and has been the subject of legislation in many jurisdictions. Greece and France have implemented to their national law the 2002/58/EC Directive on privacy and electronic communications according to which, the consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website.

4. Fields of processing of personal financial data

Before studying the legal protection of personal financial data, it would be useful to make an indicative reference to the aspects in which we «meet» personal data of economic behaviour.

The e-commerce is the most common example. It consists of the buying and selling of products or services over electronic systems as well as the exchange of data to facilitate the financing and payment aspects of the business transactions. The main advantage of e-commerce is that the sale and purchase transaction is completed electronically and interactively in real-time. For the transaction's accomplishment, the appropriate software is needed in order to permit the electronic data interchange (EDI) between the parties that participate to the said transaction (Sinaniotis-Mavroudis -Farsarotas, 2005). This interchange is the structured transmission of data between organizations by electronic means. It is used to transfer electronic documents from one

computer system to another (Maisl,1996), as for example from one trading partner to another trading partner.

The most characteristic forms of e-commerce are the web banking, the electronic auctions as well as the distance marketing of financial services. A general framework to cover certain legal aspects of electronic commerce in the internal market was provisioned by the directive 2000/31/EC which has been implemented to Greek law by the presidential decree 131/2003 and in French law by the law 2004-575. The use of computers and telecommunications to enable banking transactions to be done by telephone or computer rather than through human interaction is called electronic banking (Giannopoulos, 2003). Electronic banking has vastly reduced the physical transfer of paper money and coinage from one place to another or even from one person to another.

Besides, electronic auctions have emerged as a major part for e-commerce, especially in Europe (Verbiest, 2000). Electronic auctions are realised with the participation of consumers and of business (business to consumer) or between the business (business to business, B2B). For the inscription on an auction site, a credit card number, a phone number and the address of the customer are needed. Moreover, in Belgium an electronic identity card is needed to enter an auction site (Wery, 2008). In Greece, doesn't exist any special legislation on electronic auctions. However the legal framework that regulates the electronic auctions is the said Directive 2000/31/EC (especially the articles 18 et seq), as well as the presidential decree 131/2003 that implemented the directive in the internal law. In any case, for this type of e-commerce the provisions for distant contracts are followed (Verbiest, 2000). In France, the electronic auctions are regulated by the law 2000-642 that implemented the said directive.

The fundamental text about distance marketing of financial services is the European Union's Directive 2002/65/EC which regulates the sale of pensions, mortgages and other financial services and products by means of distance communication, which includes sales taking place on-line or by e-mail, telephone, fax or regular mail. In this Directive, significant terms are defined such as: distance contract, distance communication, financial service, supplier, consumer, and means of distance communication. Directive's main goal, is to encourage competition between suppliers throughout Europe and its' member states. Many financial services, such as banking, credit, insurance, personal pensions, investment or payment services, lend themselves to being sold at a distance, with consequent cost and access benefits for consumers and sellers alike. The Directive also aims to ensure that consumers using distance sales channels are not at a disadvantage to those using the more traditional sales channels. The consumer should have confidence in the security of the transaction, which in turn should lead to increased use of new technology for the sale and purchase of financial services. In Greece the directive above was implemented to national law by the law 3587/2007 and in France by the decree 2005-1450.

Another field where the processing of personal financial data takes place is the e-government. E-government is called the use of Information & Communication Technologies (ICTs) to make public administrations more efficient and effective to the people who need to use them (ec.europa.eu/information_society/activities/egovernment). ICTs are already widely used by government bodies, just as in enterprises, but e-government involves much more than just the tools. E-government enables all citizens, enterprises and organisations to carry out their business with government more easily more quickly and at lower cost.

In the European Union's internal market, people are able to move freely-either for work or for other reasons-and consequently they have to be able to deal with public services are to provide significant added value to citizens and business, then it is crucial that different government bodies, both within a country and in different EU member states, are able to share information easily and co-operate in serving citizens.

E-government, enables individual to proceed in transactions with public services, in order that he arranges fast and safely all these matters that concern his economic, tax, professional or

property situation.The Lisbon Strategy on 2000 as well as the treaty of Lisbon, were the main texts that regulated the e-government.

In Greece, an e-government example is the on line tax declaration to the general secretariat for information systems of the Ministry of Economic and finance (www.gsis.gr), the on line submission of ownership declaration to the Hellenic Cadastre (www.ktimatologio.gr), as well as the online application for the pension and insurance matters via site of Citizen's Service Centers (KEP, www.kep.gov.gr). Similarly in France, where the term electronic administration (administration électronique) is preferred instead of e-government, the citizen has the ability to submit on line his tax declaration (www.impots.gouv.fr) and be informed for it in real time, to pay on line fines issued by automated traffic enforcement cameras (radars) and all fines where the payment counterfoil contains an e-payment reference (www.amendes.gouv.fr) as well as to make an on line application for the granting of family allocation of social security (www.caf.fr).

5. The regulatory framework of personal financial data's electronic processing in banking sector in Greece and France

Before examining the legal framework of personal financial data's electronic processing in banking sector in Greece and France, it would be useful to make some general remarks on personal data's protection in these two countries. Despite the fact that till 1995 almost all the member states of European Union, had in their national legislations laws and other official texts about the protection of individual's privacy, the first fundamental legal text regulating the processing and the legal protection of individual's personal data (including personal financial data) was the Directive 95/46/EC about ''the protection of individuals with regard to the processing of personal data and on the free movement of such data''.

This Directive (almost known as the European Data Protection Directive), gave to member states the guidelines for implementation to their national law. Thus, in compliance with the Directive, personal data means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to, should be taken into consideration. The processing of personal data means any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction. A personal data filing system means any structured and stable set of personal data that are accessible according to specific criteria. The data subject of a processing of personal data means an individual to whom the data covered by the processing relate.

Greece implemented the said Directive by voting the law 2472/1997 and France the law 2004-801 which amended the law n°78-17 of 6 January 1978 on data processing, data files and individual liberties. According to the Directive's provisions (see article 8 case 1 of 95/46/EC), the financial data are considered to belong to the category of the simple data and not to this of the sensitive ones, despite the fact that they refer to a strictly private field of individual's life. The reason that justifies this discrimination is the need for transparency and for fight of money laundering that probably couldn't be satisfied if a special status of protection would have been recognized to this category of personal data (Igglezakis, I., 2003).

In Greece, according to the amendment of article 2 case b of law 2472/1997 by the article 18 par.1 of law 3471/2006, the list of ''sensitive'' called personal data has been restricted. While in the former legal framework the participation in any kind of association was considered to be

sensitive data, after the law's amendment the ''sensitivity'' of the data lies to the fact that only the trade-union membership is considered as a sensitive datum (Alexandropoulou-Egyptiadou, 2007), for example the participation in a union of adopted children or nephritic persons. This is the example of a Public Service which grants benefits and financial privileges to special categories of citizens, such as homeless, unemployed or disabled persons. After its decision, the Public Service publishes (or uploads on the internet in its website) the results and the names of the beneficiaries.

In case of infringement of the provisions of the above mentioned legal framework, administrative, civil and penal sanctions must be imposed.

In order to better understand the regulatory framework of personal financial data's electronic processing in banking sector in Greece and France, we have to examine the function (interbanking information systems), the principles according to which the data are being processed, the data's recipients as well as the individual's concerned rights during the data's processing.

5.1 Interbanking information system in Greece

In Greece, an interbanking company named TIRESIAS (www.tiresias.gr) processes data that reflect the economic behaviour of individuals and companies as well as data that contribute to the prevention of fraud in financial transactions. Members of TIRESIAS' system are all the Greek Banks which entrusted it with the development and the management of a reliable Credit Profile Databank. The data stored in TIRESIAS' system, contribute to the protection of credit, the reduction of credit risk and the improvement of financial transactions, to the benefit of individuals and the banking system in general. The correct estimation of the solvency and the financial credibility of banks' clients contribute to the decrease of the bad debts resulting to the decrease of cost of loans and of the citizens' debts.

TIRESIAS operates based on the principle of respect and protection of public rights and abides by law 2472/97 on the ''Protection of the individual from the processing of personal data'' and the relevant provisions of the said Directive 95/46/EC. Due to the fact that the credit profile data of individuals is of personal nature, their processing is subject to the relevant provisions of Law 2472/97. However, this data's category doesn't belong into the ''sensitive data'' category, as defined in the above law as we have already seen. TIRESIAS' system has adapted the development and operation of the Credit Profile Database and the Risk Consolidation System, in order to assure the individual's protection from the processing of such data. TIRESIAS' system organised personal financial data in four files called "systems":1. The Default Financial Obligation System (DFO) & Mortgages and Prenotations to Mortgages System (MPS), 2. The Credit Consolidation System, 3.The lost or stolen Identity Card and Passport System (IPS) and 4. The Terminated Merchants System (TMS).

5.1.1 The Default Financial Obligation System (DFO) & Mortgages and Prenotations to Mortgages System (MPS)

This system contains data (e.g. bounced checks, liquidation auction announcements, bankruptcies) concerning the credit behaviour of individuals and companies. Both DFO & MPS aim at supporting a more accurate assessment of the financial credibility of the clients (current or future) by the banks. The Mortgages Prenotation to Mortgages System contains the respective data for mortgages and prenotations.

5.1.2 The Credit Consolidation System (CCS)

This system contains data concerning consumer and housing loans, credit cards of natural persons and credit to small and medium-size businesses (with annual revenue less than 2,5 million Euro). It contains information about the status of the credit (current balance with no delinquency, delinquent balance etc). The function of the Databank and all the relevant activities secure the regular collection of data from credit/financial institutions regarding possible debts from loans, their processing, the completeness control as well as the dissemination of the processed information. The access to this file is possible with the consent of the interested party. In the case of consent withdrawal, a relevant indication is presented, that is evaluated by the bank.

5.1.3 The lost or stolen Identity Card and Passport System (IPS)

This system is an auxiliary Databank containing declarations (submitted either directly to TIRESIAS or via the Ministry of Citizen protection) of lost or stolen ID cards and passports. The purpose of this database is to keep, the wider banking sector in general, informed in order to protect transactions and clients involved from potential consequential damages resulting from loss or theft.

5. 1. 4 The terminated Merchants System (TMS)

This system contains information about merchants whose contracts for accepting credit cards as means of payment have been terminated by the acquiring banks. The termination of these contracts takes place due to reasons related to fraudulent activity. The database does not include sensitive information concerning card usage or their owners' personal data. This file aims to contribute to the protection of credit provided by banks and assuring reliable financial transactions. This purpose is attained through the provision to financial institutions of access to the database previously mentioned, therefore enabling them to evaluate risks undertaken while signing a contract with a specific merchant. Access to this database is provided for private use to the departments of credit institutions and payment card operators that are authorized for signing contracts concerning card acceptance with merchants.

5.2 Interbanking information system in France

In France, the Bank of France (www.banque-france.fr) organized its filing systems containing personal financial data and reflecting individual's economic profile in order to evaluate the trustworthiness of banks' clients and protect them from personal debt problems. These filing systems operate and process clients' personal data according to the provisions of the law 78-17 as it was amended by the law 2004-801. To accomplish this mission, the Bank of France has provided a secretariat for the household debt commissions. The commissions, set up in each French département (that is an administrative unit), are charged with finding solutions to the problems encountered by individuals who have incurred excessive debts or who experience financial problems due to unforeseeable events. According to the law 2003-706, the commission may, depending on the gravity of the financial difficulties faced by the debtor, direct the case: i) either towards an out-of-court procedure based on the negotiation of an agreed repayment schedule liable to be accepted by the debtor and his creditors or ii) towards a personal recovery procedure - based on personal bankruptcy procedures - when the debtor's situation is ''irremediably compromised''. In its role as administrator of the household debt commission secretariats, the Bank of France is charged with receiving debtors' applications and processing their cases, notably

by conducting, on the commission's behalf, negotiations with creditors and drawing up recommendations to be submitted to the courts.

For the said purpose, the Bank of France created and operates under its control: 1.The Central Cheque Register (FCC), 2. The National Register of Irregular Cheques (FNCI), 3.The National Database on Household Credit Repayment Incidents (FICP) and 4. The National hotline for lost or stolen cheques (CNACPV).

Moreover, CNIL has authorised several subsidiaries of banking groups, specialized in consumer credit (such as Credit Agricole in 2005 with Finaref and Sofinco; BNP Paribas in 2006 with Cetelem and Cofinoga) to share data on their borrowers for purposes of bad debt prevention, based on five criteria: a. the legitimacy of purpose: for example the prevention of fraud and bad debts, b. the occasional and restricted nature of data exchanges between the credit institutions, no centralized database is created. Client records kept by the institutions cannot be fuelled with any data transferred via the query system, c. the quality of institutions granted authorization to exchange data, when all are consumer credit specialist companies, hence all bound by the banking secrecy, d. the existence of a shared financial risk between these institutions, reflected in an effective control by certain companies over others, or in third-party risk management and e. the explicit authorization given by the client to share data covered by the banking secrecy, requiring among other that the client be clearly informed of the purposes and recipients of the shared data.

However, CNIL hasn't authorized other institutions which couldn't fulfill the above mentioned criteria (e.g. the case of the companies Experian and Infobail).

5.2.1 The Central Cheque Register (FCC)

The Central Cheque Register, created in 1955 as a result of the public authorities' and banking industry's desire to encourage the use of cheques by making them more secure. The law 91-1382 on the security of cheques and payment cards, amplified the Bank of France's role in the prevention of the issuance of bad cheques. The legal provisions relating to cheques and, more specifically payment incidents have been incorporated in the French Monetary and Financial Code (Articles L. 131-1 et seq). The Bank of France keeps a central record of payment incidents involving bad cheques, bank-imposed bans on writing cheques that are systematically imposed on account holders that causes these incidents, and court-ordered bans on writing cheques.

5.2.2 The National Register of Irregular Cheques (FNCI)

The National register of irregular cheques (FNCI) centralises bank details on: all accounts opened by persons banned from writing cheques, stop payment orders resulting from loss or theft of cheques, account closures and the characteristics of counterfeit cheques. According to the article L.131-86 of the French Monetary and Financial Code, the Bank of France is responsible for providing information on the regularity of all cheques that it is likely to accept in payment of goods and services. The banks transmit this information to the FNCI in accordance with the provisions of Article L. 131-84 of the Monetary and Financial Code and Articles 19 and 28 of Decree 92-456 of 22 May 1992. The FNCI also centralises reports of loss or theft of chequebooks made by victims to the National hotline for lost or stolen cheques. These reports are kept for 48 working hours after which they need to be confirmed by a stop payment order from the bank that holds the account.

According to the provisions of the Article 4 of the Decree of 24 July 1992, the Bank of France has entrusted a private company with the task of implementing FNCI consultation

procedures. The service that gives access to the FNCI is called VERIFIANCE-FNCI- Bank of France. In order to consult the FNCI, the users must scan the «CMC7 strip», that is the magnetic strip that is located at the bottom of the cheque. Various colours transmit various types of information to retailers: Thus, the green colour means no information in the FNCI, the white colour means that the cheque can't be read, the red colour, means that the cheque is irregular (that is ban on writing cheques, closed account, stop payment order due to loss or theft, counterfeit cheque), the orange colour means that the bank account is under a stop payment order due to loss or theft (with no indication of cheque numbers) or a report to the National hotline for lost or stolen cheques.

5.2.3 The National Database on Household Credit Repayment Incidents (FICP)

The FICP was created on 1989, in accordance with the provisions of the Act of 31 December1989 on Preventing and Resolving Personal Debt Problems that have already been incorporated into the Consumer Protection Code under Articles L 333.4 to L 333.6 The system is organised around household debt commissions with at least one for each department (department is the French administrative unit). These commissions work with the creditors of people facing debt problems in order to try to achieve out-of-court agreement and reschedule the debts. If all this procedure fails, the debt commissions can propose specific measures that will be binding on the parties, following approval by the judge that handles the case.

The FICP's primary aim is to provide credit institutions with information that will help them assess the repayment difficulties encountered by individuals. The Article L333-4 of Consumer Protection Code defines the content of the database. That is: a. the payment incidents about non-professional loans to individuals b. applications filed with the debt commissions, c. mutually-agreed or court-ordered work-out measures to deal with cases of overindebtedness, including the personal bankruptcy measures (Act 2003-710 of 1 August 2003) and d. the civil bankruptcy rulings made in the Alsace and Moselle departments.

In fact, the National database on household credit repayment incidents (FICP), administered by the Bank of France, is the key tool in the prevention of overindebtedness. Being listed in the FICP does not prevent credit institutions from granting loans, but is designed to provide them with information so that they can better assess their risks in this area of activity.

The FICP records this information for persons who stay in metropolitan France, the overseas departments and Saint Pierre and Miquelon. It also collects information on French citizens who stay outside France in respect of non-professional loans. Since 1st April 2007, the rules of the Regulation 90-05 (amended) of 11 April 1990 have been applying to the overseas units of New Caledonie, French Polynesie, Wallis and Futuna and the territorial unit of Mayotte.

5.2.4 The National hotline for lost or stolen cheques (CNACPV)

The National hotline for lost or stolen cheques was set up by the Bank of France in 1996. It is open 7 days a week and 24 hours a day and allows cheque book holders to report the loss or theft of cheque books to the National Register of Irregular Cheques (FNCI) by telephone, as soon as the incident occurs, and, most importantly, when banks are closed. Once the report is recorded in the FNCI, an alarm is set off should the lost or stolen cheque be scanned by a retailer that subscribes to the VERIFIANCE-FNCI-Banque de France service (it is the service which permits the access to

the National Register of Irregular Cheques, www.verifiance-fnci.fr), the FNCI consultation system. Reports are deleted after 48 working hours if they are not confirmed by stop payment orders issued by the account holding bank and reported to the FNCI. Account holders must therefore transmit written stop payment orders to their banks as soon as possible in accordance with the provisions of Article L 131-35 of the French Monetary and Financial Code.

5.3 The operational principles applied during personal financial data's processing

In order to be lawfully processed the financial data must be collected first of all fairly and lawfully for specific, explicit and legitimate reasons in view of such purposes according (article 6 of law 2472/1997 and of law 801-2004). In our case, banks' purpose for processing personal financial data is the minimization of the risks involved while signing credit contracts with uncreditworthy clients, as well as the minimization of the creation of doubtful debts, in the protection of commercial credit as well as in the improvement of economic transactions **(principle of scope)**. The data processing is justified as ''absolutely necessary'' for the achievement of the said purpose, while the protection of commercial credit compared with the interests of the data subjects, may be considered to ''evidently prevail'' over them, in the sense of Art. 5, par. 2, section e, according to the DPA'S decision No 109/1999 repeated by the DPA'S decision No 24/2004. Consequently, processing is allowed even without the consent (Alexandropoulou-Egyptiadou, 2007) of the data subject, provided that the latter has been informed (Art. 11, par. 1 and Art. 24, par.3, Law 2472/1997).

Additionally, data, subject to processing, concerning purchasing and selling of real property, must not be processed as they are found to be incompatible with the principle of proportionality, according to which data «must not be excessive in relation to the purposes for which they are processed at any given time» in compliance with the Art.4, par.1, section b Law 2472/97 (Alexandropoulou-Egyptiadou,2004) and article 6 par. 3 of the law 2004-801. Maintenance of such data in advance for an indefinite number of persons who do not have (and maybe never will) any contractual relation with banks far exceeds the purposes of the file (**principle of proportionality**). Processing of the above mentioned data is allowed only with consent of the data subject.

Besides, in order to be lawfully processed the personal data must be accurate and where necessary kept up to date. Especially in the banking field where the individual's data are kept in specific files with long storage time, controllers must be more attentive, for example, when the name of the individual concerned is very common e.g. Papadopoulos, the controller must add further identifying elements such as mothername, date of birth, etc. However, the only responsible part to update the individual's data status is the controller (**principle of accuracy**) in case that the new elements, as for example payment of debt, result of a public file (Alexandropoulou-Egyptiadou, 2004). On the contrary, if the new elements (e.g. payment of debt) don't result of a public file, then the person concerned must inform the controllers about the change of data's status.

Moreover, the personal data shall be stored in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed **(principle of respect of storage time),** as it will be presented in the following paragraph.

5.4 Storage time of personal financial data

One of the most important aspects of the protection of personal financial data is their maintenance and their storage time in the individual's reference file by the controllers. The directive 95/46/EC as well as the text of Greek and French law about the protection of personal data, remind the principle that a data's processing can last for a period during which the controller intends to carry out data processing or maintain the file (article 6 section e of laws 2472/1997 and 2004-801). According to the 95/46/EC Directive, art. 2 d, controller shall mean 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; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

Of course, it is another matter, if historic, statistical or scientific reasons lengthen the personal data's storage time, because of the fact that these data aren't related to a particular subject. The nature of the economic personal data, signals it's duration in the reference file. That means for example, that according to the article 3 of the recent law 3816/2010 in Tiresias' system the bounced checks' and unpaid bills of exchange are stored for two years, the liquidation auction announcements' and the confiscations and seizures' are stored for four years, the bankruptcies are stored for ten years and at the same time Mortgages, Prenotations of Mortgages, conversions of prenotations to mortgages' storage time expires when these are wiped out.

Similarly, in French interbanking information system if the debt commission finds that a debtor's situation is permanently impaired, it may direct the case towards personal bankruptcy proceedings, which are recorded in the FICP for eight years (L 332-11 Consumer Protection Code). Moreover, once debtors have fully repaid creditors named in mutually-agreed or court-ordered measures, these work-outs must be deleted from the database immediately. With the exception of the partial cancellation of debts, personal recovery procedures and personal bankruptcy measures can be rescinded at any time, provided that the debtor supplies proof of full payment of the sums due from each of the creditors concerned. According to the Cnil's recent position, the storage time has to be reduced for certain categories of data (data concerning overindebtedness), from ten to eight years.

The data's storage time, not only for the personal financial data but for the personal data in general, is based on the right to oblivion (or the right to forget) that protects an individual's privacy and stop him from being permanently held to ransom by unguarded actions from his past.

5.5 Recipients of personal financial data

Recipients, are considered to be the persons to whom data are expected to be communicated to during the collection stage. In greek as well as in french information banking system, only banks, financial institutions, credit card companies and public sector entities are justified to be recipients of data, in consistence with the purpose of the processing. On the contrary, third parties in economic transactions and non-parties are not justified to be recipients of such data. It is self-evident that only the above recipients of personal data have the right to use them. Further processing, transfer to third parties etc. is completely prohibited. TIRESIAS must comply with the obligation to inform the data subject (see article 24 par. 3 in combination with the Art. 11, par. 1 of the Law 2472/1997). Especially, in greek interbanking information system, factoring and leasing companies are also recipients (DPA's decision No 523/1999). On the contrary, insurance companies which insure credits aren't considered to be recipients (DPA'S No 62/2003 decision).

The data subject has to be informed during the collection stage about the recipients, as well as about the addition of other recipients or of another category of recipients a posteriori (after the

data collection) shall, in accordance with the Law, be subject to the provision of Art.11 of law 2472/1997 and 11 of law 2004-801, resulting in the obligation of the Controller to inform the data subject . It has to be mentioned that there is an obligation for the Controller to inform about every specific transfer made by him when asked by the recipient.

5.6 Individual's rights on his personal financial data's processing

As we have already seen, according to the articles 11 of law 2472/1997 and 32 of law 2004-801, the Controller must, during the stage of collection of personal data, inform the data subject in an appropriate and express manner of the following data about his identity and the identity of his representative, if any, the purpose of data processing, the recipients or the categories of recipients of such data as well as about the existence of a right to access. According to article 2 d of the Directive 95/46/EC, 'Controller, shall mean 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; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

If the Controller, in order to collect personal data, requests the data subject's assistance, he must inform him specifically and in writing. By means of such notification the Controller shall also inform the data subject whether he is obliged to assist in the collection of data, on the basis of which provisions, as well as of any sanctions resulting from his failure to co-operate. When it comes to the Controller's obligation for the information of a considerable number of persons, then the information can be done via the medias of press by dispensation of the general rule of in concreto information (Alexandropoulou-Egyptiadou, 2004).

Apart from the right of information, the individual whose personal data are being processed or have been processed has also the right to access to his data (see the article 12 of the law 2472/1997 and the article 39 of the law 801-2004). As to this the Controller must answer in writing, undue delay and in an intelligible and express manner: All the personal data relating to him as well as their source, the purposes of data processing, the recipient or the categories of recipients, any developments as to such processing for the period since s/he was last notified or advised, the logic involved in the automated data processing, the correction, deletion or locking of data, the notification to third parties, to whom the data have been announced, of any correction, deletion or locking taken that the notification is not impossible or does not demand disproportionate efforts. The right of access is exercised by means of a relevant application to the Controller. All persons may obtain information pertaining to them by going in person to customer service and information offices. Persons wishing to contest and, where appropriate, amend database information in their name, must submit a request to the reporting institution either by physical presence to the bank or by post .

Besides all the above, the individual has also the right to object (see the article 13 of the law 2472/1997 and the article 38 of the law 801-2004) at any time to the processing of data relating to him. Such objections shall be addressed in writing to the Controller and must contain a request for a specific action, such as correction, temporary non-use, locking, non-transfer or deletion. Moreover, any person shall be entitled to declare to the Authority that he does not wish data relating to him to be submitted to processing in order to promote the sale of goods or long distance services. The Authority shall keep a register for the identification of such persons.

6. Conclusions and final thoughts

The new ethics that brought the technology's progress was the reason that changed the ''legal spirit'' about individual's privacy and economic behaviour. Conservative or not, the fundamental European texts as well as the Greek and the French national legal framework remind us the challenge of balancing between the maintenance of technology development and the protection of individual's private life. In this study, it is obvious that national and european legal framework (including the decisions of National Data Protection Authorities) try to get the balance right between the banks' (credit enterprises') profits and their clients' rights.

It is sure, that the regulatory framework concerning the processing of personal financial data can be developed and be more complete in case that on the one hand the citizens-bank clients have the sensibility to appeal to the Data Protection Authorities and on the other hand the banks show their interest to resolve daily problems (coming from this processing), often with the help of the abovementioned Authorities. Additionally, it would be crucial for the whole matter of protection of personal financial data, the enactment of special and detailed guidelines coming from the Data Protection Authorities (soft law). As a result, the function of the banking system will be defined and the transactions' security will be improved. Moreover, an important step to personal data's protection could also be the enactment of a law concerning not only the natural persons but also the moral ones, given that the companies consists the majority of banks' customers.

REFERENCES

A. Books and papers (on line) :

1. Girot, J.L.(2005): ‘’Le harcèlement numérique’’, DALLOZ, page 60
2. Chatillon, G. (2007) : ‘’Les données personnelles : enjeux juridiques et perspectives IDT juin 1999’’, dimanche 13 mai 2007, online at : www.georges-chatillon.eu/accessed 14.06.2010 : ‘’constituer des «méga-bases de données comportementales’’ouvre la voie au marketing efficace et lucratif’’.
3. Igglezakis, I.(2003) : ‘’The legal framework of e-commerce’’, Sakkoulas, Athens-Thessaloniki, page 211
4. Sinaniotis-Mavroudis, A.-Farsarotas, I. (2005): ‘’Electronic banking’’, Ant. N.Sakkoulas, Athens-Komotini, , pages 114-116
5. Maisl, H. (1996) :’’Le droit des données publiques’’, L.G.D.J,page 51
6. Giannopoulos, G. (2003): ‘’Internet Banking –Legal questions about internet banking transactions’’, Internet Banking Legal aspects, Deltion of Hellenic Bank Association, 3 rd semester, page 97, online at: www.hba.gr/accessed 14.06.2010
7. Verbiest, T.(2000): ‘’Les ventes aux enchères électroniques : quel cadre juridique ?’’, article of 1/10/2000, online at: www.droit-technologie.org/actuality-344/les-ventes-aux-encheres electroniques-quel-cadre-juridique-chroni.html/accessed 14.06.2010
8. Wery, E. (2008) : ’’Première mondiale : le site belge d'eBay utilise la carte d'identité électronique pour authentifier les utilisateurs’’, article of 28/02/2008 online at:http://www.droit-technologie.org/actuality-1123/premiere-mondiale-le-site-belge-d-ebay-utilise-la-carte-d-identite-e.html /accessed 14.06.2010
9. Igglezakis I. (2008): «The Information Law», Sakkoulas, Athens-Thessaloniki, page 211
10. Igglezakis, I.(2003): ‘’Sensitive Personal Data’’, Sakkoulas, Athens-Thessaloniki, page 94
11. Alexandropoulou-Egyptiadou, E (2007).:‘’Personal Data-The legal framework of their electronic processing‘’, A.N. Sakkoulas, Athens-Komotini, page 33-34, ref. 15
12. Alexandropoulou-Egyptiadou, E.(2007):‘’Personal Data-The legal framework of their electronic processing‘’, A.N. Sakkoulas, Athens-Komotini, page 57 et seq.
13. Alexandropoulou-Egyptiadou E (2004): ‘The electronic processing of personal data in banking field-The legal framework’, Armenopoulos, page 1377
14. Alexandropoulou-Egyptiadou, E (2004): ‘The electronic processing of personal data in banking field-The legal framework’, Armenopoulos, page 1391

15. CNIL's paper : ''Vers une réforme crédit à la consommation et des fichiers de crédits'', 26 mai 2010, on line at : www.cnil.fr/dossiers/argent/actualites/article/238/vers-une-reforme-du-credit-a-la-consommation-et-des-fichiers-de-credits/ accessed 14.06.2010
16. Alexandropoulou-Egyptiadou E (2004): 'The electronic processing of personal data in banking field-The institutional framework', Deltion of the Hellenic Bank Association, page 30
17. Alexandropoulou-Egyptiadou E (2004): 'The electronic processing of personal data in banking field-The legal framework', Armenopoulos, page 1391

B. Legal texts and decisions (on line):

1. Law 2472/1997: Official Gazette: A΄ 50/10.04.1997
2. Law 2004-801: JORF of 7.8.2004
3. Law 78-17: JORF of 7.1.1978, page 227
4. Law 3471/2006 : Official Gazette A' 133/28.06.2006
5. Loi 2005-862 : JORF n°175/9.7. 2005, page 12357, text n° 16
6. 2002/58/EC Directive: Directive on privacy and electronic communications, online at: http://eur-lex.europa.eu/ accesed 14.06.2010
7. Directive 95/46/EC: Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, online at: http://eur-lex.europa.eu/ accessed 14.06.2010
8. Directive 2000/31/EC: Directive on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Official Journal of the European Communities on 17.7.2000, L 178 pages 1-16
9. Decree 131/2003: Official Gazette A΄ 116/16.05.2003
10. Law 2004-575: LOI n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF n°143 of 22 June 2004, page 11168
11. Law 2000-642: JORF n°159/11.07. 2000 page 10474
12. Directive 2002/65/EC: Directive concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC, online at: http://eur-lex.europa.eu /accessed 14.06.2010
13. Law 3587/2007: Official Gazette A΄ 152/10.07.2007
14. Decree 2005-1450: Décret n°2005-1450 du 25 novembre 2005 relatif à la commercialisation à distance de services financiers auprès des consommateurs. On line at : www.legifrance.gouv.fr /accessed 14.06.2010
15. Lisbon Strategy: http://europa.eu/scadplus/glossary/lisbon_strategy_en.htm /accessed 14.06.2010
16. Treaty of Lisbon: http://eurlex.europa.eu /accessed 14.06.2010
17. Law 2003-706: JORF n°177/2.8.2003, page 13220

18. CNIL's decisions of 8 March 2007 and of 10 July 2007 (Experian and Infobail case) on line at: www.cnil.fr
19. Law 91-1382 on the security of cheques and payment cards: JORF n°1/1.1.1992, page 12
20. Decree 92-456: JORF n°120/23.8.1992, page 6985
21. DPA'S decision No 109/1999 repeated by the DPA'S decision No 24/2004:www.dpa.gr/decisions /accessed 14.06.2010
22. Law 3816/2010: Official Gazette A' 6/26-01-2010