E-Commerce: The e-Consumer and the attacks against the personal data

By Nomikou Eirini
Attorney at Law
Master Degree in Web Law

1. Introduction

Private life is a rather broad concept. Social and technological changes have made a precise definition of this notion extremely difficult. At the beginning, the concept of private life was defined as being all that opposed to public life, but the borders between these two parts of our life are not always so clear. Thus, in the 50's, according to Dean Nerson, private life consisted of "a personal sector, held, in order to be inaccessible to public, without the will of the interested party, whatever constitutes the necessary parts of personality: the right to intimacy". In this direction, family life was also added. A little later, jurisprudence adds that "each one has the right to oppose to any intrusion in the intimacy of his private life and to place limits on what can be published about it» [TGI Paris, 4 mars 1987, JCP 1987 II 20904, note E. Agostini].

Through the evolutions of private life, certain elements seem to be constants of private life and through them, it will be able for this concept to be defined. Thus, one can distinguish three categories: First of all, body intimacy, like sexuality, nudity, health, maternity, death. Then, all that affects personal life, like family life, sentimental life, religious life, financial life and finally whatever permits the identification of a person, like the name, address, image…

In the United States, the Dean William Prosser systematized the jurisprudential tendencies and proposed a categorization in four parts of the right of private life: 1) Intrusion upon a person's seclusion or solitude, or into his private affairs; 2) public disclosure of embarrassing private facts about the plaintiff ; 3) publicity which places the plaintiff in a false light in the public eye et 4) appropriation for the defendant's advantage, of the plaintiff's name or likeness. But the technological developments are able to show us that these traditional categorizations, mentioned above, are insufficient and inadaptable to the technological development. The information society poses new aspects to the notion of private life and demands a widening of the traditional notion of private life. From a wider point of view, private life protects the person as it guarantees a liberty of action, expression, prohibiting any physical attack in order to safeguard human dignity.

As a result of the above, the notion of private life, according to the article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms appears insufficient compared to the new elements added to the notion of private life. In 1981, the adoption by the Council of Europe of the Convention for the

Protection of Individuals with regard to Automatic Processing of Personal Data remains till nowadays and in this field, is the only constraining legal instrument on international level, with universal vocation. This Convention defines a certain number of principles so that the data are collected and used in a loyal and licit way.

At the same time, in 2000 the European legislator wanted to support the development of Internet and the use of numerical means, in order to eliminate the barriers between people. As a result, the Directive of June 8, 2000 is adopted, and it is the directive concerning the electronic commerce. With this directive the aim is to frame the electronic commerce which is defined: as the operations which consist of selling goods and services online, and the purely dematerialized exchanges and certain nonpaying online services proposed to consumers and aim to have a commercial purpose. The Community legislation focuses on carrying out an internal market, which will be homogeneous and will allow economic operators to offer their services to consumers of various nationalities. That is possible with the Internet, a mean which can abolish the geographical and linguistic obstacles, and as a result can improve competition in a Common Market. However, it is essential that this right is developed in a protected environment. It requires enacting protective rules for the consumer, which will help the safe exploitation of the various online services. Within the efforts of development of an internal market and the movement of people and goods within the EU, it appears vital to harmonize the national legislations for the processing of data, concerning the private life. A trans European flow of personal data requires a uniform protection. In this direction European Union presents the Directive 95/46/CE of the European Parliament and the Council of October 24, 1995 concerning the protection of individuals, with regard to the processing and free movement of personal data. According to the previously mentioned directive about data processing, as personal data can be defined: "(…) any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; ".

The consumer, throughout the online transactions is threatened by several attacks to the various aspects of his private life to the profit of companies, which use more and more new marketing tools in order to gain customer's loyalty, by proposing services according to the analysis of their online behavior. Throughout this paper, the various forms of attacks to the private data of consumers will be examined.

2. Dangers of the private life of consumer during the different contract phases

i. During the precontractual phase

During internet operations, the consumer can quickly become victim of techniques which, can collect personal data, that will be able to be used for a usurpation of identity. The usurpation of identity can be defined as the act of taking the control of the virtual identity of a person, by stealing the password and the means

of identification in order to use the account as if the thieves are the authorized persons, at various purposes, often fraudulent.

The usurpations of identity generally aim at committing a penal offence in order to derive an economic advantage from this action. They try to obtain the credit cards' number or to collect information, which will make it possible for the defrauders to act and answer the questions of identification requested by most of the sites. For example at the time of an online purchase, elements of marital statuses are required, as well as numbers of credit cards. The goal of the collection of information is to overcome without difficulty, the obstacles of safety of Internet sites. A great number of identities had been usurped in order for the thefts to be able to carry out purchases online. According to the Federal Trade Commission, 9,3 million Americans were victims in 2004 of a usurpation of identity, like the usurpation of an existing or not credit card and a bank account. The usurpation of identity requires the accumulation of two basic actions: collection of personal information and the use or exploitation of this information.

The most common methods which can also affect the cyber consumer, are: phishing, pharming and spoofing.

a. Phishing

The Phishing is the most common phenomenon, which threatens a great number of companies. It is a method of "social engineering", consisting of exploiting not a data-processing fault, but a "human fault". According to the general Commission of terminology and neology it is the "Technique of fraud aiming at obtaining confidential information, such as passwords or numbers of credit cards, by means of messages or sites usurping the identity of financial institutions or trade companies". It begins with an email which persuades the user to reveal personal data by imitating a website of a real company.

It results from the English term phishing and it is a spelling variant of the word fishing. It was invented by the "pirates" who tried to steal the accounts of the American company AOL and it comes out from the English expression password harvesting fishing: an attacker presenting himself as a member of AOL team and sending an instant message to a potential victim.

The principal goal of the data-processing criminals, who use phishing, is the money theft. The most popular targets are the online banking services, and the auction sites of sales such as eBay or Paypal. Typically, the messages sent, seem to emanate from a company worthy of confidence and are formulated so as not to suspect the recipient and consequently carry out an action. The common approach is to indicate to the victim that the account was deactivated because of a problem and that the reactivation will not be possible unless the victim takes certain action. The message then provides a hyperlink which directs the user towards a Web page that resembles the real company page worthy of confidence. When arriving at this misleading page, the user is invited to provide the website with confidential information, which is recorded by the criminal.

b. Pharming and spoofing

The two other techniques of usurpation of identity are parts of the attack of the man-in-the-middle (often abbreviated MITM) which add a condition according to which the attacker has the possibility not only to read, but also to modify the messages. The cryptography is used by the pirate in order to read, address and modify encoded messages between two parts, by making them believe that they are talking directly to each other over a private connection. The pharming is a technique of usurpation of identity that consists of an act of hacking the domain name system. The author of this act pirates the domain name. The customer of the bank selects the web address of the bank in order to proceed to operations at his bank account. As the domain name has been pirated, the customer is redirected to a false site similar to the one belonging to the bank and gives his personal and confidential information. It can be carried out by means of a malware, reconfiguring the network parameters of the equipment of the infected computer.

The spoofing is an alternative technique, which consists in pirating IP addresses of a machine, in order to have free access to it. That is done by using malevolent software, of viruses or Trojan horses, in order to integrate in an information system and recover personal data.

In order to protect the consumers from these types of attacks, the countries' legislators try to implement legislations in order to restrict the phenomenon. On June 16,2005 the president of the United States signed a law named "Identity Theft Penalty Enhancement Act", which aims at weighing down the duration of imprisonment against the thefts of numerical identity and also concerning the intellectual property: "The Digital Millennium Copyright Act of 1998".

In Greece, there is no jurisprudence concerning phishing websites and as a result, neither the judge nor the legislator, have presented any legal aspects of this fraudulent act. The "phishing" could be sanctioned on the base of the infringement of fraudulent collection of personal data envisaged by the Greek law 2472/1997.

In addition, in order to persuade the victim the pirate uses the identity of the pirated site. It uses for example the trademark of the site, its graphic charter and its contents. It thus counterfeits the trademark and the rights of intellectual property of the creator of the original website.

In the majority of cases, the main goal of the pirate is the cheat. One could mention at this point the first judgment for phishing in France by the TGI of Paris on the 2/09/2004. A student in BTS computer studies tried to cheat by representing at a website, which he had registered in Germany, the certified copy of the home pages of the Crédit agricole and Crédit Lyonnais banks in order to collect banking information and to transfer sums from clients' accounts. Hence, he fraudulently reached the system of automated processing of data of one of the banks and managed to modify the data contained in this system, carry out two transfers of a total amount of 15.800 euros and visit more than ten accounts. Fortunately, after the customers' complaints the bank locked the transfer system very quickly and the transfer of the funds could not take place. He was condemned to one year imprisonment with deferment and to more than 11.000 euros of damages for attempt of cheat, modification of data resulting from a fraudulent access to a system of automated process and fraudulent access to this system.

Another possible intention of the pirate can be the use of the identifiers in order to reach the private part of a site, or an Intranet.

c. Cookies

The use of cookies is another way of collecting of personal data, used especially by the companies, in order to collect information concerning the interests of consumers. For the French organization for the protection of personal data, CNIL, a cookie file indicates "a recording of information by the server in a textual file, located on the customer's computer, information which only this server can have access to and modify them later on". The cookies are installed on the hard disk of the compluter of the user, when the customer consults certain sites. They make it possible to record traces of navigations of the user on certain sites, and store information concerning the practices and preferences of the internet surfer via his computer. At the time of the following visit to that site by the user, all the data of the cookie are repatriated towards the site, which installed the cookie so as to be exploited. The Cookie file contains information and data which will be likely to identify the internet surfer every time he is connected to a Web site. This information could be the domain name where the cookie was emitted from, the expiratory date of this Cookie, etc. Thus, the cookie stores information like: date and visiting time of the user, answers collected via an on-line form, personal information collected by the server. Cookies can also be used to check the effectiveness of the design of a site and the marketing used by the site. These are the temporary cookies which do not record any permanent data and which remain in the Random-access memory of the computer.

The majority of the recent navigators make it possible for the users to decide if they accept or reject the cookies. The users can also choose the storage period of cookies. However, it is possible that the complete rejection of cookies makes certain sites unusable, like the shopping baskets of e-shops or sites which require a connection using identifiers (user and password).

Consequently, one can notice that cookies cause important attacks to the private life and the anonymity of the users of the Web. In general, cookies are returned to the server which installed them to our computer or to a server which belongs to the same domain name. These cookies are called tracking cookies. Moreover, the web pages that we visit can contain images or other elements, belonging to other sites. The cookies which are set up during the recovery of these external components are called third party cookies. These include cookies coming from the undesirable pop-up windows.

The companies of publicity as well as the companies of direct marketing and "one-to-one marketing" use third-party cookies in order to track the users through various sites which they visit and on which they put cookies. This way, companies know and categorize preferences, practices, reflexes, tastes and interests of a user who could become a future consumer, create a profile and direct them personalized publicities thanks to spamming. This practice can be considered as an intrusion to the consumers' private lives and therefore, texts of law have been adopted by the Members of the EU.

The directive 2002/58/EC of the European Community of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector, contains rules about the use of cookies. Particularly, the article 5, paragraph 3 of this directive demands "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 processing, and is offered the right to refuse such processing by the data controller». However, article 5 of the directive 2002/58/CE also states that the storage of data for technical reasons is exempted of this law. According to this directive the cookies «can be a legitimate and useful tool, for example, in analyzing the effectiveness of a website's design and advertising, and in verifying the identity of users carrying out on-line transactions. Where such devices, for instance cookies are intended for a legitimate purpose, such as to facilitate the provision of information society services»

According to article 5 of the directive, the Member States of the European Union must guarantee the confidentiality of communications carried out by means of a public network of communications and services of electronic communications accessible to public, as well as the confidentiality of the traffic data and the relative ones. "In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so".

In order to frame the use of the cookies, the directive states that:

"However, such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment".

According to this provision, the consent of the user is necessary in order to install cookies on the hard disk. It is also necessary that the reasons for which these cookies will be installed are indicated. Moreover, the directive requires that the information transferred to the hard disk is clear, precise and show the finality of the recording of such cookies.

It is interesting to mention the case of a company of online-profiling "Double Click" in the United States and the charges made against it by consumers [United States District Court for the Southern District of New York,154 F. Supp. 2d 497; 2001 U.S. Dist. LEXIS 3498, March 28, 2001, Decided]. Indeed, when an internet surfer visits one of the 13.000 Web sites for the first time, on which Doubleclick has installed advertising banners, a unique number of identification

"GUID" is allotted. This number is installed in a file cookie. When the internet surfer revisits this site, it reads its "GUID and the data which have been recorded by the cookie, and records its identifying code in a giant data base on which certain information such as the names of the visited sites, the key words of the pages of the visited sites and the personal data, which are necessary to carry out an order, to seek schedules of transport etc is attached.

The complaint was mainly based on the following federal laws: (**1**) *Electronic Communications Privacy Act* (*ECPA)* which punishes the data-processing hacking (**2**) *Wiretap Act*, which contains general prohibitions related to the interception of telecommunications; and finally (**3**) *Computer Fraud and Abuse Act*, which prohibits the unauthorized access to an information processing system, as wells as some laws of States. The problem in this case was that the federal laws aim at the protection of the information processing systems, whereas the laws of the States aim at the protection of private life. As a result, this judgment did not make it possible to advance jurisprudence on this point, because "when federal claims are dismissed, retention of state law claims under supplemental jurisdiction is left to the discretion of the trial court". Consequently, the Judge did not come to a conclusion about the protection of private life, but he resent the parts in front of a judge of a State.

To conclude, another way of collecting personal data, which can threaten the consumers throughout their electronic operations, is by a software which automatically collects electronic addresses on Internet sites. The absence of conservation of addresses excludes the collection within the meaning of this provision. On the other hand, even if there is conservation of data, there is no unfair collection because "the express consent of the interested party that intervenes a priori or a posteriori, is not required as such by the law in order to characterize the loyalty of the collection".

d. Email marketing and spamming

An important attack to the private life of consumers is made by the unsolicited commercial communications and the spamming. According to a study of the European Commission published in 2010, called "towards cross-border sales and consumer protection", during the last 12 months, 6 out of 10 consumers in the European Union were victims of commercial communications and not requested offers.

The use of the email for direct prospection is not subjected to this law, if the interested party gave preliminary consent on the system called "opt in". This consent must be expressed within a direct and personal contact and not dissimulated under various conditions. The legitimacy of the use of email at ends of direct prospection requires that the information data of the interested party were obtained in a legitimate way conforming to the directive 95/46/EU, within the framework of the sale of a product or supply of services. These emails can concern products or similar services, after having informed the person so that there is the right of opposition to these commercial communications (rule of opt out). The customers must always be clearly informed when their personal information is used this way. Moreover, according to article 13.5 of the directive 2002/58/CE provides that "Member States shall also ensure, in the framework of Community law and applicable national legislation, that

the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected" and that they take measures so that the service providers regularly check the registers of opt-out addresses.

The Directive provides that the solicited commercial communications must be presented as such and they do not have to be dissimulated in another e-mail or message, nor under a false identity, answer or a wrong number. The transmitter of the commercial communication must be clearly identifiable as well as the address, so that the person who receives the emails can ask for suspension with simple means and without expenses.

On European level, the directive 2005/29/CE contains a general clause concerning the general prohibition of unfair commercial practices which intends to replace the divergent general clauses, which already exist in the Member States and remove any barriers of the internal market. It describes two principal categories of unfair commercial practices, the "misleading" and "aggressive" practices by taking into account the average consumer. In conclusion, there is also a black list, which contains the list of practices which, under all circumstances, will be regarded as unfair and prohibited - without the test of average consumer having to apply.

In Greece, spam is regulated by the article 11 of the Law 3471/2006, which incorporated in the national law the Directive 2002/58/EU, about the protection of personal data and private life in the sector of electronic communications. Spamming is frequently used by advertisers, but it is also a way of online or one to one marketing, which makes it possible for the companies to approach directly, quickly, and massively the internet surfers without any cost for the transmitter. On the other hand, it also attacks the private life of consumers, who can be misled.

e. Insufficient information on behalf of the person in charge of the data processing

In various sites which exist on Internet and make it possible to carry out electronic transactions, one can be misled rather easily, because of the lack of information given by the person who benefits from a service or the salesman of products.

According to the article 5 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), "the service provider shall render easily, directly and permanently accessible to the recipients of the service and the competent authorities, at least the following information:(a) the name of the service provider;(b) the geographic address at which the service provider is established;(c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;(d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;…"

Nevertheless, many service providers do not provide all this information. For example they indicate a false company name, or they do not provide their postal address. As a result, the cyberconsumer can be misled, and not only never receive the product or service ordered, but they can also face a fraudulent use as of their personal data, provided within the framework of a purchase (like the data concerning his bank card), without having neither the right nor the possibility of recovering these data or identifying the supplier in order to be able to make a complaint against him.

ii. During the contractual and post-contractual phase

a. On line Authentication

The majority of service and product providers on the Internet, in order to facilitate the purchases of their customers, propose the creation of a clients' account. In this account, one can add data which is necessary so as to carry out an electronic operation and reach the account that is already created at a site and carry out a purchase without having to fill these data again. The difficulty which arises here is that, one can very easily create such a profile, but it is much more difficult to remove it, because many providers ask for a mail in order to be able to remove these profiles and the data which composes them.

The cyber-traders also, put electronic portfolios at the disposal of the consumer. This technique allows the automatic memorization of a customer's bank card number in the clients' account, so that he does not need to fill it in every time he makes a purchase. As a result, this practice accelerates the phase of payment and supports the impulse purchase, purchases into 1 click, without having time to reflect.

This online authentication gives the cyber-traders the possibility of recording a customer's preferences, in order to propose him personalized offers. There are sites, which also require information, concerning family, age, elements which do not have any relation with the facilitation of purchase. Moreover, a great number of consumers are not informed yet, and they do not check the legal mentions concerning the private life of the sites they visit for their purchases. Then they become victims because their data can be used for several purposes and processed without their consent. Moreover, although it is prohibited, these operators sell the data to companies of direct marketing or use them at purposes incompatible with the initial objective. The European law always offers the possibility to the national authority of the data protection to give the right to repair any undergone damage, because of the illicit treatment of data. The problem is that this treatment is done without initially informing the consumer.

On the other hand, another problem which often arises is the theft of these accounts. The experts of the cyberspace steal the passwords and the identifiers of these clients' accounts with which they have the capacity to carry out transactions on behalf of the customer and with his bank card.

b. Abusive terms

The abusive terms are defined at the Greek Law by the article 2 of the Law 2251/1994 for the protection of consumers. The law provides that abusive are the terms that have as a result the perturbation of balance of rights and obligations of the contracting parties and finally the damage of the consumer.

In the contracts concluded within the framework of the electronic commerce, there can be clauses which also attack the private life and the personal data of the consumer. According to the Recommendation n°07-02 of the Commission of abusive clauses in France, related to the contracts of sales of products concluded by the Internet: "considering that several general conditions confer to the service/product provider the right to communicate to thirds, whose identity is not specified, personal data concerning customers so that they can address a direct prospection to them; even if we believe that the consumer has in a general way granted the diffusion of the personal data for a direct prospection by electronic way, such a stipulation causes a significant imbalance to his detriment". The Commission in the recommendation, supports that in contracts of electronic commerce, it is necessary to eliminate the clauses having for object or effect "to consider given the consumer's consent for diffusion to any partner, not identified by the provider of the service or product, of the personal data in order to address by electronic way a direct prospection to the consumer".

Moreover, in the analysis made by the Commission of the abusive clauses on the judgment of the Court of Paris, on April 5, 2005 [Tribunal de Grande Instance de Paris, Jugement du 5 Avril 2005] , one can notice that "the clause which provides the professional with the right to remove the inbox and its contents in case of prolonged inactivity of the subscription or if those were not consulted, is abusive since it allows the unilateral modification of the characteristics of the service offered without notice". Also, "the clause which provides that the use of services, like the telephone number of the consumer, or the use of personal data of identification, is abusive as it makes the consumer automatically responsible for any use of the service, even in the absence of any fault on his part. As a result it deprives him of the possibility of proving the fraud which he could be the victim of and exempts the professional of his own obligations in the event of failure of his service or his material". Finally, the clause which provides "the use by the subscriber of the email at fraudulent or harmful ends, such as the mass mailing of not solicited messages and other in the type of "spamming" are formally prohibited" as abusive in what they leave to the professional a discretionary capacity to appreciate if the mass mailing of not solicited messages rises from the practice of "spamming" whereas the aforementioned sending can have a legitimate reason".

In particular, it is interesting to evoke the judgment of the Court of Nanterre on June 2, 2004 [Tribunal de Grande Instance de Nanterre, le 2 Juin 2004] concerning the Company AOL Bertelsmann Online France and the "Union Fédérale des Consommateurs Que Choisir" (UFC), as far as certain clauses in the contract of access to Internet in its drafts published in 2000 and on 28/01/03 are concerned. The court

regarded as abusive the clause of the contract in question which stipulates that: “Your personal data will be transferred, treated and stored at the United States and in the European countries, by AOL, AOL lnc. and their affiliated companies (“companies of group AOL') (…) so as to reach your personal data.” Moreover, another clause specified that: “We can preserve personal data relating to your online purchases by our group or of commercial thirds” and in fine “However, the companies of the AOL GROUP will be able to use these data to make known to you products or services likely to interest you” or “for direct marketing”. Even the later version of this contract was regarded as abusive according to which “Your personal data will be transferred, treated and stored at the United States and in other countries, by the companies of AOL group which will reach your personal data by installing certain functions necessary for the supply of the AOL service, and this, by ensuring the respect of the protection of personal data and of their transfer, in accordance with the applicable law”. Subparagraph 2 contains the same precision: “We can preserve personal data related to your online purchases by our group or by commercial thirds”.

The UFC supported that such clauses are abusive because they create an imbalance in the direction of article L 132-1 of the Code of Consumption; “it makes it possible for the AOL company to distribute the personal data of its subscribers to marketing services, which will analyze their behavior, or will use them as targets, and recalls that only an expressed agreement of the subscribers can authorize the AOL company to transfer the personal data towards other companies, and this according to the European Directive of July 12, 2002(…).”

Within the same framework, the Court of Paris on October 28, 2008 also regarded as abusive the clauses of this kind concerning the personal data and their uses without the express consent of the consumer.

c. Transfer of the data of consumer to third countries

The greatest threat for the consumers and the collection of their personal data is the transfer of these data out of the European Union and towards countries without protection equivalent to the one of the European Union. These are the countries which did not transpose in their national law the directive 95/46, within the framework of the European Free Trade Association (EFTA) or for which there is not the Decision of the Commission related to the observation of the adequate character of the data protection in third countries. The danger also lurks in the transfer of data towards companies to the United States, which do not make party of the device known as “Safe Harbor”. It is about a voluntary self certification on behalf of companies established in the United States which adopt a series of principles of personal data protection and protection of private life, published by the ministry of trade of the United States.

In general, people whose data are likely to be transferred, must be informed about this transfer according to the directive for the protection of personal data. They must be informed in a sufficiently detailed way about the finality of the transfer, the country of establishment, the recipient of data and if this country does not grant an adequate protection within the meaning of the European directive 95/46, the categories of recipients of the data and, if necessary, the nature of assured protection

of the transferred data. On the contrary, what happens when the data, which consumers gave within the framework of these electronic transactions, are transferred without the previous notification of the person concerned? How can we be sure that even in this case data are protected from any illicit treatments?

Article 25 of directive 95/46 provides that the responsible for a treatment cannot transfer personal data towards a State not belonging to the European Community, unless this State ensures a level of protection adequate or sufficient, for the private life, freedoms and basic rights of people with regard to the processing of their personal data. Moreover, persons who intend to transfer personal data are obliged to make known, the decisions of authorization of transfer of personal data to the European Commission and the European supervisory authorities. In this way, it can be ensured that people are provided with protection as far as the processing of their data are concerned when they leave the European territory so as to be the subject of a treatment out of the European Union.

The transfer of data towards a third country constitutes any communication, copy or displacement of data via a network, or any communication, copy or displacement of these data from a support to another, whatever the type of this support is, insofar as these data have vocation to be the subject of a treatment in the recipient country.

Moreover the article 26 of the directive provides that:

“By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

d. The particular case of credit cards

A substantial and fundamental element of electronic transactions is the payment by electronic means. The electronic payment is the payment of an amount of money by the debtor but with an additional speed. For instance, we could evoke the "electronic wallet" which is kind of plastic money with which one stores a preset amount of money and uses it for purchases. This dematerialized currency can be directly transferred with a software installed on the computer of a consumer or in a smart card. This means of payment removes the posteriori relations with the bank. Moreover, the traditional credit card is the means of payment usually used and at the same time holds the highest risk when it comes to the danger of frauds.

On the contrary, posting on a Web site a document to be printed, completed and given to the bank or the handing-over of an amount of money followed by its deposit on a bank account does not constitute an electronic payment, because the notion of electronics is in the process and not in the payment stricto sensu.

The electronic tools of payment include personal data at purposes of payment and other related operations and allow the identification of people as well as the traceability of transactions, the operations made using plastic money.

The problems which arise with the credit cards appear at the time of identification of the card or the user, the authentication of the transaction and its traceability. It is the moment where the customer will be invited to compose his personal code on the keyboard of the terminal or the telephone. One could also evoke the case of partnership between banks which use information of bank accounts of their customers for commercial purposes. As a consequence, there is again the possibility of collection and processing of data which must be declared at the Data Protection Authority of each country, satisfy the obligations of safety, the confidentiality, the respect of finality of treatment, and the information of people, but also respect their rights of access, correction and opposition.

On the other hand, this identification makes it possible for the tradesmen to propose services according to the preferences of the clients, known by their traces throughout their purchases. Customers' files are created, with the purpose to find all information concerning the consumer-customers and make a behavioral segmentation. These files can also be yielded, rented or put at disposal on a purely free basis, transforming in this way the data collected into a true economic value.

Moreover, banks especially, create files known as of exclusion or "black lists" with index information related to the incidents of payment but also to penally reprehensible behaviors. These treatments must also be object of declaration at the data protection authorities.

Furthermore, a great number of the incidents of accounts' thefts appeared the moment the banks gave the possibility of transferring money and carrying out

transfers via their site on the Internet. Many consumers were victims of thefts of their accounts, because their computer was pirated or because they did not pay sufficient attention, so as to avoid malevolent actions and as a result saw their account empty, and their money sums transferred everywhere in the world.

It is also necessary to evoke the great importance of transfer of banking data towards the United States. It is interesting to examine the position of the French CNIL and the European CNILs (G29) concerning this transfer and particularly concerning an agreement under the negotiation which gave access to the United States to the intra-European banking data stored by SWIFT, on the new server installed in Switzerland. SWIFT is a co-operative company which offers to the banks a protected system of messaging to the banks. These data are related to the amount of money of a transaction, the currency, the name of the one who receives the money, the customer who asked the financial transaction and his financial institution.

In June 2006, the American authorities set up a system of surveillance of the international banking transfers forwarded by the company SWIFT. This action initially caused the reactions of G29 which on November 22, 2006, gave an opinion concerning the conditions of provision of European data, stored in the United States in the base SWIFT. According to the G29, these transfers are opposite to the European principles of data protection, but the negotiations for the necessary guarantees so as to ensure this transfer still continue. As a consequence, one can notice that the great economic powers continue to attack the private life of consumers and within the framework of certain operations, even European Personal Data Authorities can face difficulties which will be solved, only after negotiations of several years.

3. Conclusion

The European legislation has established the principle according to which any individual has the right to private life. However, this freedom and right to private life became fragile and threatened in a place where the information systems multiply, the notion of "national" which frames the borders and the limits of a country disappear, the universality settles in more and more aspects of life, with an evolution of technology which presents an astonishing acceleration. The legal authorities lose the control of protection, because the applicable law on the cyberspace is not obvious anymore and it does not always ensure the same protection.

The European Union framed the protection of personal data, and the Member States protect this right as a basic right. But why do the majority of cyber consumers hesitate to carry out transactions outside the national level? Article 14 of the directive 2000/31/CE of the European Parliament and the Council of June 8, 2000 related to the electronic commerce in the internal market frames the responsibility of the host for illicit activities or information. As a result, if after the notification to the host of the illicit contents of a website, the malevolent site of e-commerce, changes host in the same country, or if it is hosted in another country in the European Union, it is always possible to chase the author of this crime between the various hosts. The problem is what happens if hosting is carried out, out of the European Union, in a country which adopts different aspects and laws about the protection of personal data, or where the freedom of expression is protected more than the protection of personal data. In this case, one cannot talk about a transfer of personal data which the European Union can

control and prohibit. Moreover, the giant companies which are located in the United States do not consider the European's Community legislation to be applicable to them.

The collection, the use and conservation of personal data could profit the consumer, because these techniques help the consumers with their electronic transactions so as to avoid repeating certain information for example when purchases are carried out. Moreover, they allow the personalization of offers suggested in profit of their economies. Furthermore, this information could be necessary for the recovery of frauds and thefts and protect the consumers from illegal practices, but also for the improvement of the services offered and the best comprehension of the needs of customers and consumers in general.

On the other hand, unfortunately the situation is not so protective of the consumer in the majority of cases. The several methods of data acquisition, the large quantity of sites universally, which try to steal the personal data of consumers, in combination with the great profit of companies by the trade and use of these data, cause concerns for the future of this situation. The fast evolution did not leave time to the legal framework to adapt to it and thus to balance cyberspace, international trade and protection of personal data.

Within the framework of this effort for consumer's protection and in order to make them feel more confident in the electronic commerce, an international co-operation is needed. The global dimension of e-commerce obliges the undertaking of measurements on a world level. The protective "guides" of OECD (1980), the convention of the Council of Europe (1981), the guiding principles of UN (1990), the European directive (1995) are not proven sufficient in the fight for the protection of personal data and private life of consumers. An international collaboration is required. An international authority which would be able to apply the protective texts worldwide and coordinate the action of the several commissions and national authorities for the protection of consumer and personal data so as to face the situation at all its extent. The universalization of trade requires the universalization of safety at the same time.

On the other hand, it is crucial that the consumers are informed. It is necessary to avoid the increase of mistrust of consumers and make them feel that they can make safe electronic transactions, by the use of new technologies, without being afraid that by doing so their personal data may be used for illegal purposes that are different from those to which they gave their consent. It is important to inform the consumers about the fraudulent attitudes, which they may face within the framework of e-commerce, but also about the ways and techniques with they can be protected by. They should be informed of their rights concerning their personal information (personal life, right of suppression, access and correction) and how to satisfy them so that they can also be in a position to control the legal uses and avoid possible attacks to their private life. A large number of consumers do not know neither the problems which they could face on the Internet nor their rights so as to protect themselves. For this reason, it is necessary that the consumers who represent the base of the pyramid are informed and that the legislations for the protection of personal life are universally controlled and applied to the suppliers of electronic commerce who control the offered services and products. In this way, the electronic commerce will be able to

extend as it was considered at the beginning by its creators. If the principal actor of e-commerce, the consumer, trusts and proceeds to electronic transactions, the E-commerce will be proved an even more fundamental factor of world economy.

References

- Iteanu O. (2008), L'identité numérique en question, Eyrolles.
- Féral-Schuhl C. (2008), Cyberdroit -le Droit à l'épreuve de l'Internet, Dalloz.
- Nerson, R. (1959), La protection de l'intimité, Journal des Tribunaux.
- Agostinelli X. (1994), Le droit à l'information face à la protection civile de la vie privée, Librairie de l'Université d'Aix-en-Provence.
- Hollande A. and Linant de Bellefonds X. (2008), Pratique du droit de l'informatique et de l'Internet : logiciels, systèmes, Internet, Delmas : Dalloz.
- Halpern C. (2003), Guide juridique et pratique droit et Internet, De Vecchi.
- Benyekhlef K. (1992), La protection de la vie privée dans les échanges internationaux d'informations, Thémis.
- CNIL (2009), Surveillance des transferts bancaires européens par les autorités américaines : vers une remise en cause des garanties négociées, Communication Commerce électronique n° 10, Octobre 2009, alerte 129.
- Prosser W. (1960), Privacy, online at http://www.californialawreview.org/assets/pdfs/misc/prosser_privacy.pdf/ accessed 01.04.2011
- Man in the middle : l'attaque par l'homme du milieu, (2007), online at http://www.journaldunet.com/solutions/0705/070524-qr-man-in-the-middle.shtml/accessed 01.04.2011
- Chawki M, « Les Enjeux des Fichiers Cookies », online at http://www.legalbiznext.com/droit/IMG/pdf/cookies.pdf/ accessed 01.04.2011
- European Commission (2010), Attitudes towards crossborder sales and consumer protection, online at http://ec.europa.eu/consumers/strategy/docs/Fl282_Analytical_Report_final_en.pdf/accessed 01.04.2011
- Europa Press Releases Rapid, Selon un rapport de l'UE, le fossé s'élargit entre transactions électroniques nationales et transfrontalières, online at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/980&format=HTML&aged=0&language=FR&guiLanguage=en/accessed 01.04.2011

- Commission des clauses abusives, « Recommandation n°07-02 relative aux contrats de vente mobilière conclus par internet, BOCCRF du 24/12/2007, online at http://www.clauses-abusives.fr/recom/07r02.htm/ accessed 01.04.2011

- « Clauses abusives : au tour d'Amazon ! », (2008), online at http://decryptages.wordpress.com/2008/11/19/clauses-abusives-au-tour-damazon/accessed 01.04.2011