SOME LEGAL AND TECHNICAL ASPECTS RELATED TO POSSIBLE INTERNET'S THREATS ON THE FUNDAMENTAL RIGHT TO PRIVATE PROPERTY

Silvia-Maria Tăbuşcă[1]
Alexandru Tăbuşcă[2]
Virgil Chichernea[3]

Abstract

Once an individual uses the modern means of payment, the credit cards, he must be aware of the possible issue that might come out. Even more, when using these "plastic money" in the online environment provided by the omnipresent world wide web one must be aware that there are enough risk involved. The commodity and easy that came with the use of the credit card also brought us new threats, new ways in which our privacy and property might be affected.

Keywords: Internet, privacy, property, cybercrime, credit card frauds

1. Introduction

During the last decade, the number of Internet users worldwide grew from 400 million in 2000 to over 5 billion users in 2010[4]. Used by such a number of people around the globe, the Internet has become, on one side, a mean by which individuals can more easily exercise their daily activities, and on the other side, it is an illusion of an anonymous and private environment. The electronic centralization of personal dates has made the right to privacy a fundamental concern of many international and national institutions. For this reason, there are many international and national legal norms which provide safeguards of fair and lawful collection, as well as of the automatic processing of personal data, imposing strict conditions on the use of this information.

Nevertheless, there are many individuals or organized groups which use personal data, especially the personal electronic contacts and, pretending that they represent an authority or a company, they collect specific personal date which may affect the right to privacy and, often, the right to property, too.

2. The right to privacy

[1] PhD Assistant Lecturer at the School of Law, ROMANIAN-AMERICAN UNIVERSITY; e-mail: silvia.tabusca@profesor.rau.ro
[2] PhD Lecturer at the School of Computer Science for Business Management, Romanian-American University; e-mail: alextabusca@rau.ro
[3] PhD Professor at the School of Computer Science for Business Management, Romanian-American University; e-mail: chichernea.virgil@profesor.rau.ro
[4] International Telecommunication Union, *StatShot No. 5*, January 2011, available from: http://www.itu.int/net/pressoffice/stats/2011/01/index.aspx

The development of the Internet removes geographical limitations to the flow of data and modern information systems, which connected with other systems, can exchange and process different personal data. Also, new developments in medical care, telecommunications, advanced transportation systems and financial transfers have dramatically increased the level of information about each person. Nowadays, nearly all countries have established some form of email interception and wiretapping over telephone and fax communications, sometimes involving thousands of illegal actions. Furthermore, the computers linked together by high-speed networks with advanced processing systems can create comprehensive dossiers on any person without the need for a single central computer system. In this global context, abuses on the right to privacy have been detected in most countries.

The right to privacy is an internationally recognized fundamental right. It is stated in the article 12 of the Universal Declaration of Human Rights[5], as well as in the article 17 of the International Covenant on Civil and Political Rights[6] which provides the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honor and reputation. The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[7] and the Organization for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data[8] are the two international instruments which promote specific legal norms concerning the protection of electronic data. Also, there are two European Union's Directives: one on telecommunication[9] and the other one on data protection[10], which provide a wider range of protection over abuses of personal data.

The right to privacy is required to be guaranteed against all such interferences and attacks whether they emanate from state authorities or from natural or legal persons. The respect of privacy requires any state to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks. The article 17 of the Covenant deals with the individual protection against unlawful and arbitrary interference. State authorized interference within the right to privacy may take place in accordance with the law. The term „arbitrary intervention" guarantees that even interference provided by law must comply with the objectives of the international norms and should be reasonable in particular circumstances[11].

---

[5] United Nations General Assembly, *Universal Declaration on Human Rights*, Paris, 10 December 1948.
[6] United Nations General Assembly, *The International Covenant on Civil and Political Rights*, New York, 16 December 1966.
[7] Council of Europe, *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data*, Stasbourg, 1981.
[8] OECD, *Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data*, Paris, 1981.
[9] European Community, *Directive 97/66/EC of the European Parliament and of the Council concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector*, 15 December 1997.
[10] European Community, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data*, 24 October 1995.
[11] United Nations Human Rights Committee, *General Comment no. 16 on Article 17 (Right to Privacy)*, Geneva, 1988.

Nowadays, especially because of the promotion of electronic commerce[12], it is generally accepted that the right to privacy of the online consumers should be threatened by their personal information which are lawful sent worldwide.

3. The right to property

The right to private property is a fundamental right of adult human beings who may not be prohibited or prevented by anyone from acquiring, holding and trading valued items not already owned by others. Article 17 of the Universal Declaration of Human Rights states that everyone has the right to own property alone or in association with others and no one shall be arbitrarily deprived of this right. Also, the International Covenant on Civil and Political Rights protects the right to property in article 5.

It has been shown that, in specific circumstances, the infringement of the right to privacy may often lead to the threat of the right of property. It usually occurs in relation to the financial institutions. The cyber-thieves steal online banking credentials. The fraudsters create fake versions of banks websites and ask users to enter their login details, which are stored and then used on the real sites.

A very clear infringement of the right of property is the unauthorized use of one's credit card credentials in order to steal his property, his money. These incidents happen more often that one should expect within our today technologically advanced and sophisticated environment.
In a recent incident, one of the most important Romanian banks (ant the last important state owned one), CEC Bank, has chosen to block no less than seventeen thousands cards and reissue them free of charge, together with new PIN and security details for each of those customers. This activity comes after a rumor of a supposed informatics attack and underlines again the utmost importance of knowing and following the rules regarding the safe usage of a banking card.

The number of valid cards in Romania, and subsequently of the number of card transactions, follows an ascendant tendency, after all the available information from the media and backed up by prestigious institutions reports, such as BNR (National Bank of Romania) itself. Following the same trend, unfortunately, more and more frauds regarding the use of credit cards appear every day. In the past, most attacks involving card transactions were based on more "classical fraudulent" means, such as finding out the PIN number of the card by use of videotaping the owner while using it or introducing a fake reading device which interfered between the card and the banking devices. These fraudulent devices were copying the relevant details before forwarding them to the appropriate banking devices but nowadays the focus shifted towards more "advanced fraudulent" means. Today, most attacks are based solely on the banking system dependency on IT systems. The modern computers help us a lot but they can also bring new levels of danger into our day-to-day transactions, based on their near "omniscience" of our banking details.

The modern credit cards were subjected to updates in mass, several years ago, with dedicated chipsets and settings in order to increase their degree of security. By default, at the time of

[12]Privacy International, *Privacy and Human Rights*, 2002, available from: http://gilc.org/privacy/survey/intro.html.

their emission from the bank, all cards have now different limitations regarding the amount of money that can be withdrawn daily from ATMs or from the bank offices, the number of operations during a certain period of time or the need to insert a different PIN number for higher amounts of money.

The tendency to use more and more online solutions for different purchases came into Romania too. Even though Romania does not have an internet penetration rate comparable to the most advanced countries, with the Nordic countries leading the way and even legalizing the use of the internet as a fundamental right written down in the constitution *(Tabusca 2011)*, our infrastructure is very new and is one of the fastest in the world even. This fact, together with the online payments that require the use of credit cards, made the tendency to use these credit cards to rise even faster.

The banking institutions emitting different types of credit cards can auto launch an alert the moment their computers see something that is out of the ordinary regarding the use of a certain card, when the card usage is not consistent with the previous usage pattern: different geographical area of usage, completely different (and higher) amounts of money, strange and repeated uses of the card for a many different transactions during a short period of time etc. Any of these issue might trigger the bank computers to block the card usage and contact the listed owner as soon as possible. Moreover, the new chip technology for credit cards makes almost impossible the process of reproducing the card details by means of unauthorized reader devices, thus greatly reducing the fraud risks (*Pirjan 2010)*.

Despite all these protection advances, the hackers are becoming more and more ingenious when addressing the credit card issue. Among the most widely spread attacks we can mention phishing, skimming and the so-called Nigerian letters.

Fishing frauds

The fishing fraud is mostly related to sending false email or SMS messages to people asking them to provide confidential information such as card number, PIN code, account number etc. These email messages are not personally addressed and, if proper and updated antivirus and anti-spam software is used, they usually end up in the Spam (or Bulk) section of the email address.

One must never follow such messages! As a rule, no bank will ever ask you to provide your confidential information by means of email.

Skimming frauds

The skimming fraud can be seen as somewhat more “hardware” type. This type of fraud involves the copying of the data from the magnetic part of the credit card by the use of special electronic devices. In order to avoid such an attack one should avoid secluded ATMs or areas with no traffic at all. The best solution is to use only devices near banking institution or inside heavy traffic areas (hypermarkets, shopping malls, boulevards etc.) and best of all, in areas supervised by video cameras. Also, one should check for any unusual devices or anything out of the ordinary regarding the ATM’s keyboard or the dedicated slot for inserting the card into

the machine; these areas are the most widely used locations for inserting fraudulent means of recording card details. Another way to increase the security degree of the card use is to never let the card out of your sight ☺. Even in restaurants, gas stations or hotels is best to oversee by yourself the paying process and always ask for the printed receipt for any transaction. Fortunately, in Romania there is almost no possibility of paying by card without personally introducing your PIN number. While this system might feel a little uncomfortable, especially when using somebody else's card – even from another family member, is best suited to customer's protection.

According to the Romanian law "the card owner is not responsible for any transaction if the electronic payment device was used without its physical presence or without its electronic identification (PIN number, access codes)[13]". This means that the bank is forced to indemnify the victim in case the fraud is made by the copying of the credit card or by its use without the solicitation for proper security codes.

Unfortunately, the credit cards issue was only specific for the Romanian market. One of the largest payment organizations in the world, VISA, is investigating a US company called EuroNet. Several thousand credit card details have been compromised by the use of a security breach in the processing company's security system.

The issue, coupled with the ongoing financial crisis that topples Europe, made break news and even the president of ARB[14] came out publicly in an interview in order to clarify the issue: "Is a problem related to the actual cards, not only in Romania but at international level. We are talking about hundreds of thousands of cards but there are no information indicating that the owners of the cards will be affected", said Mr. Radu Gratian Ghetea[15].

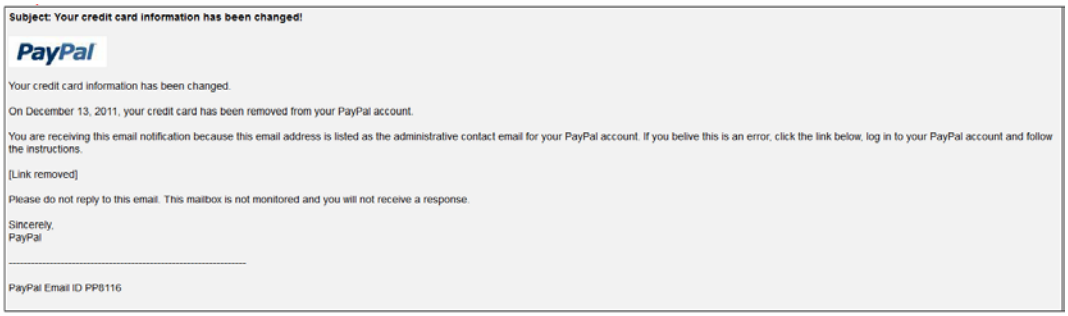
Nigerian letter

The Nigerian letter frauds are based on email messages sent in order to inform people about supposed winnings of diverse prizes. After the normal congratulations for your good luck, they also request some of your personal banking details in order to finalize payments for taxes usually. All these messages are usually labeled as "confidential" or "urgent" and they are not, of course, personalized. Although most specialists consider these messages as a completely stupid way to try to cheat someone, every year there seem to be quite enough people that believe such rubbish and throw their money on illusive future gains.

According to FBI studies published in 2011, there is a rate of about 2 people out of 1000 that fall for these scams. The amounts of money lost by the victims are usually between 20 and 20000 US dollars.

At international level, December 2011 brought another cyber-crime to the public attention. The world reputed PayPal company was the victim of an e-mail scam. Thousands of PayPal customers received a seemingly valid email message during the month of December 2011:

[13] See Art.25(1) from the Romanian National Bank Regulations no.6 from 2006
[14] ARB = Romanian Banks Association
[15] President of ARN, President of CEC Bank, Associate Professor with the Romanian-American University



Subject: Your credit card information has been changed!

PayPal

Your credit card information has been changed.

On December 13, 2011, your credit card has been removed from your PayPal account.

You are receiving this email notification because this email address is listed as the administrative contact email for your PayPal account. If you belive this is an error, click the link below, log in to your PayPal account and follow the instructions.

[Link removed]

Please do not reply to this email. This mailbox is not monitored and you will not receive a response.

Sincerely,
PayPal

PayPal Email ID PP8116

People who felt for the ruse and followed the link were taken to a fake "PayPal" website that has been carefully designed to mirror the genuine PayPal website. The casual observer might find it difficult to notice any difference between the fake webpage and the real PayPal site. If the victim went ahead and entered his or her login details on the fake webpage, a following web form was displayed. The form asked for the victim's name, address, contact details, and driver's license details as well as his or her credit card information.

The threat was considered serious enough to provoke an official response from PayPal. The official company website developed an entire section dedicated to the issue of phishing and PayPal even published a list of thing that "PayPal will never ask you in an email":

"To help you better identify fake emails, we follow strict rules. We will never ask for the following personal information in email:

- *Credit and debit card numbers*
- *Bank account numbers*
- *Driver's license numbers*
- *Email addresses*
- *Passwords*
- *Your full name"*[16]

All information submitted on a bogus website - including the user's PayPal login details - can be collected by the cyber-criminals operating this scam campaign. Once they have collected these information from their victims, the wrong doers can then use it to login to his or her real PayPal account, steal more personal information and make fraudulent PayPal transactions. They can also use the stolen personal and credit card information to commit credit card fraud and identity theft.

Besides these most common privacy and property threats that were encountered in Romania during 2011 and the world scale PayPal scam, we should also mention the top ten of such cyber-crimes investigated at international level.

Upon analyzing the reports of several hundred organizations involved in electronic security, investigators from the Bright Hub organization[17] managed to deliver such a top of threats categories:

[16] https://www.paypal.com/au/cgi-bin/webscr?cmd=xpt/Marketing/securitycenter/general/UnderstandPhishing-outside
[17] http://www.brighthub.com/

1. Non-delivery (paying online for products or services that fail to be delivered)
2. Auction fraud
3. Debit and credit card frauds
4. Confidence fraud (also referred to as advance fee fraud)
5. Computer fraud (password and credentials theft)
6. Check fraud
7. Nigerian letter fraud
8. Identity theft
9. Financial institutions fraud
10. Data security and integrity threats

4. Conclusions

It has been often argued that there is no right to privacy once the individual uses the Internet and its online services, and that this fact must be clearly stated and understood. However, it depends on each of us, in the exercise of our own personal responsibilities, to take care of our own privacy.

At this moment, there is no national or international organism or institution that can regulate this field of activity and defend the people's right to privacy. Unfortunately, the individual and the society as a whole must make an effort and educate itself in these topics. The best way to avoid being caught in such unpleasant situations is to study first, to ask the others for advice about what you are trying to do, talk to others before corresponding with a "millionaire" stranger on the internet, search the web for information about a company that promotes products at huge discounts, phone the bank if you receive an e-mail requesting your personal credit card credentials, change your PINs and passwords on regular basis and do not use obvious information. In more special situations, call security professional help – the money you spend this way might save you a lot more comparing to what you might lose to the cyber-criminals of the 21st century.

Bibliography

Pirjan, Alexandru. "Electronic commerce security in the context of the means of payment dematerialization." *Journal of Information Systems & Operations Management* (Editura Universitara) 4, no. 1 (May 2010): 184-194.

Tabusca, Silvia Maria. "The Internet Access as a Fundamental Right." *Journal of Information Systems and Operations Management* (ProUniversitaria Publishing House) 5, no. 1 (May 2011).

International Telecommunication Union, StatShot No. 5, January 2011, available from: http://www.itu.int/net/pressoffice/stats/2011/01/index.aspx;

United Nations General Assembly, Universal Declaration on Human Rights, Paris, 10 December 1948;

United Nations General Assembly, The International Covenant on Civil and Political Rights, New York, 16 December 1966;

Council of Europe, Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, Strasbourg, 1981;

OECD, Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data, Paris, 1981;

European Community, Directive 97/66/EC of the European Parliament and of the Council concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 15 December 1997;

European Community, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, 24 October 1995;

United Nations Human Rights Committee, General Comment no. 16 on Article 17 (Right to Privacy), Geneva, 1988;

Privacy International, Privacy and Human Rights, 2002, available from: http://gilc.org/privacy/survey/intro.html.