Boccella, Nicola; Misuraca, Riccardo; Tudisco Thor, Pierpaolo

Article

The protection of personal data

International Journal of Technology for Business (IJTB)

Provided in Cooperation with:
University of Economics in Bratislava, Faculty of Commerce

Suggested Citation: Boccella, Nicola; Misuraca, Riccardo; Tudisco Thor, Pierpaolo (2020) : The protection of personal data, International Journal of Technology for Business (IJTB), ISSN 2644-5085, Springwish Publisher, Bratislava, Vol. 2, Iss. 1, pp. 43-54, https://doi.org/10.5281/zenodo.3894480

This Version is available at:
https://hdl.handle.net/10419/260669

Volume: 2 Issue: 1 ISSN: 2644-5085

SPRINGWISH PUBLISHER

International Journal of Technology for Business (IJTB)

The Protection of Personal Data

Nicola Boccella [1], Riccardo Misuraca [2*], Pierpaolo Tudisco Thor [3]

University la Sapienza of Rome, Italy [1], University Europea of Rome, Italy [2, 3]

Abstract

With the exponential growth of digitization and electronic market, personal data has taken on a key role for all individuals actively involved in the process. Any type of transaction, from the payment of a product or service to registration on a web site, requires extensive use of information and personal data. In this paper we will analyse the process of collection and transmitting personal data from a practical and regulatory point of view. In particular, after describing the nature and principles governing their dissemination, the paper analyses the main stages that European regulation has taken over time. The aim is to analyse the behaviour that companies and consumers must adopt in order to ensure compliance with current legislation. In addition, the paper deals with the different systems of attacking personal data by hackers and the respective countermeasures that can be taken by companies to protect their customers.

Keywords: Personal Data, Privacy, General Data Protection Regulation, European Union, Cyber Crime

1. Introduction

In the field of electronic commerce, where every day many different kinds of transactions are executed, personal data of existing consumers is often transmitted without regular supervision. Frequently, enterprises violate and publish information without an express authorisation of owners. It means that, personal data, might be used improperly, both for advertising purposes and to transmit them to third parties. For this reason, entrepreneurs or creators of websites should take care of the protection of personal data, both in the interest of their customers and in order to avoid legal consequences. The goal of the legal framework is to avoid such infringements by ensuring consumers an adequate protection and by constantly monitoring existing activities in digital transactions.

*This is to indicate the corresponding author.
Email address: riccardo.misuraca@libero.it
First Online: 10 June 2020
DOI: 10.5281/zenodo.3894480

In recent decades, new types of companies have originated. These companies earn through the transmission and exchange of personal data, an activity that represents their main source of revenue. These aspects had to be more controlled because, today, personal data can be considered as property. For this reason, and following the progressive growth of digital market, authorities have expressed the need to strengthen the legislation for the protection of personal data at European and national level (Lynskey, 2015).

1.1 What is personal data?

Personal data means all information related to the identity of a person. It could be an expression of his physical, physiological, genetic, psychic, economic, culture and social identity. It includes (Business Insider, 2019: Pizzetti, 2017)

- Name, date of birth, address, nationality;
- Tax code;
- Bank data;
- IP address, cookie, geolocation data;
- Gender and skin, hair and eye color;
- Property;
- Online customer data;
- Training and professional certificates;

In the circumstances, when we talk about personal data we refer to all those data or information that directly or indirectly can be associated with a natural or legal person. Non-personal data, instead, is information collected anonymously and cannot be used to identify a specific person. It could include visitor data on certain website or other non-specific information. Such non-personal data is not regulated by law, for this reason entrepreneurs or traders can use this type of data to compile statistics or user profiles without prior consent or authorization of owners as the Data Protection Act establishes (Orofino et al., 2018; Kuner, 2012).

Data analysis is also very relevant in online marketing because information can be used to create advertisements and to promote products tailored to a single user and their needs. The new European General Regulation clearly establishes to what extent personal data can be collected in the context of e-commerce. In general, the prohibition is subject to authorization. This means that before using any data, it is necessary to carefully check for each individual case on whether it is permitted by law and if it is necessary to obtain the explicit authorization of the respective user. This is particularly appropriate for the so-called "personal data of particular categories", which include, inter alia, ethnic and cultural origin, all political, religious and philosophical opinions as well as genetic data and biometric (Treccani, 2019).

Furthermore, all entrepreneurs must be aware about the necessary conditions to collect and use personal data of users. In general, to perform these activities, three specific principles must be respected: purpose limitation, data minimization and transparency.

Purpose limitation

This principle states that the collection and exploitation of data is allowed only for the use or purpose clearly expressed in the contract. As soon as the contract or use process is terminated, the entrepreneur is obliged to immediately and completely delete all personal data. An extension of this requirement is allowed only if the data is still needed for billing. The transmission of personal data to third parties is not allowed except for invoices or criminal proceedings initiated by authorities.

Data minimization

The second fundamental principle is data minimization. It means that each entrepreneur or web site should only collect as little customer data as possible during a transaction. The registration of user within a certain platform can be made anonymously where this doesn't affect the purchase of the product. When this is not enough for providing the product or service, customers are required to indicate only the mandatory information or data explicitly requested for the use of service.

Transparency

This is one of the most important principle in the field of data protection. It states that it's necessary to inform each customer about the methods of collection, use, consultation or other data processing and how data are processed and will be processed in the future. The explicit consent of the user to the storage and processing of data provided, in accordance with the purpose limitation is fundamental. It means that firms not only must record the consent, but also ensure that the customer can revoke it at any time in the future.

1.2 Risks and possible measures for protecting user privacy

The lack of compliance with fundamental principles and the consequent violation of client's rights can generate very high penalties. The European regulation provides high fines up to 20 million euros or 4% of a company's annual turnover. Administrative offenses are in particular those that are committed intentionally or through negligence, such as:

- Hide the sender or the commercial nature of the message
- Inform the user incompletely about the type of data collection, or not informing
- Not promptly delete personal data
- Report a user profile to the data relating to the bearer of the pseudonym

In addition to claims for damage, the person concerned is also entitled to compensation. Internet universe is composed of a great ramified structure with global coverage and a very high transmission speed. It means that any type of data can reach every corner of the planet within a fraction of a second, generating extraordinarily communication benefits. However, when data transmission is uncontrolled, it could be very dangerous for the owners. The law, therefore, has the duty to keep up with the time to guarantee the maximum protection of personal data, even if the speed with the technologies evolve certainly doesn't facilitate the task. Ideally, we should aim for a collaboration between marketing and law. Companies should not abuse their powers and respect the privacy of customers, in doing so the former can gain long-term customer trust (European Union, 2019).

This research is interested to analyze how the regulation concerning the collection and processing of personal data has changed over time at European level, identifying not only the crucial historical steps with which it evolved, but also any differences between national and European regulations. Moreover, our interest has been to describe how the regulatory framework governs activities of the single person, consumer or seller of goods and services, operating within the digital market.

2. Regulations on the processing of personal data: European rules

Our societies are increasingly digitized. The speed of technological developments and the way in which personal data are processed in the light of these changes have a daily impact on each of us in various ways. Recently, the legal frameworks of the European Union (EU) and the Council of Europe protecting the privacy and personal data have been revised. In the field of data protection, the EU and the Council of Europe have introduced wide-ranging and sometimes complex reforms, with a wide range of benefits and repercussions for individuals and businesses alike (European Union, 2019).

Europe is at the forefront of data protection worldwide. EU data protection rules are based on Council of Europe Convention 108 and EU instruments, including the General Data protection regulation, the data Protection Directive for police, judicial authorities (Orofino et al., 2018).

There are numerous rights related to the processing of personal data that have been introduced into European jurisdiction, going back to the salient points we can consider (Pizzetti, 2017: Carey, 2018):

- Pursuant to Article 8 of the ECHR, the right to protection with regard to the processing of personal data is part of the right to respect for private and family life, domicile and correspondence
- Convention No. 108 is the first, and to date the only, legally binding international instrument dealing with data protection. The Convention was the subject of a modernization process, which was completed with the adoption of the Amending Protocol on 18 April 2018
- EU law has recognized data protection as a separate fundamental right. This is enshrined in Article 16 of the Treaty on the Functioning of the European Union and in Article 8 of the Charter of Fundamental Rights of the EU
- EU law first regulated data protection through the Data Protection Directive in 1995
- In the light of rapid technological developments, the EU adopted new legislation in 2016 to adapt data protection rules to the digital era. The General Data Protection Regulation became applicable in May 2018, repealing the Data Protection Directive
- General regulation on data protection, the EU adopted legislation on the processing of personal data by state authorities to combat crime. Directive (EU) 2017/680 lays down data protection rules and principles governing the processing of personal data for the purposes of the prevention, investigation, detection and prosecution of criminal offences or the enforcement of criminal sanctions.

Data protection in Europe began in the 1970s with the adoption of legislation by some States to control the processing of personal data by public authorities and large companies. Data protection instruments have therefore been created at European level and, over the years, data protection has evolved to a distinct value, which cannot be classified as a right to privacy. In the EU legal order, data protection is recognized as a fundamental right, distinct from the fundamental right to privacy. This distinction raises the question of the relationship and differences between the two rights. The two rights are different in terms of wording and scope. The right to privacy consists of a general prohibition of interference, subject to certain criteria of public interest which may justify interference in certain cases.

The protection of personal data is seen as a modern and active right, establishing a system of checks and balances to protect individuals whenever their personal data are processed. The processing must comply with the essential elements of the protection of personal data, namely independent control and respect for the rights of the data subject. From 1995 to May 2018, the main legal instrument of the EU in the field of data protection was Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (Data Protection Directive). It was adopted in 1995, at a time when several Member States had already adopted national laws on data protection and arose from the need for harmonization to ensure a high level of protection and the free flow of personal data between Member States. The Data Protection Directive has established a detailed and comprehensive system of data protection in the EU.

In accordance with the EU legal system, the directives do not apply directly and must be transposed into the national law of the Member States. Inevitably, Member States have a margin of discretion in transposing the provisions of the directive. This has led to the creation of diverse data protection standards in the EU and different interpretations of definitions and standards in national legislation. The levels of implementation and the severity of sanctions also differed across Member States. Finally, since the preparation of the Directive in the mid-1990s, there have been significant changes in information technology. Combination of these reasons is at the heart of the reform of EU data protection legislation. The reform led to the adoption of the General Data Protection Regulation in April 2016 Directive 680, after years of heated discussions. Such discussions on the need to modernize EU data

protection rules began in 2009, when the Commission has carried out a public consultation on the future legal framework concerning the fundamental right to the protection of personal data.

The proposal for a regulation was published by the Commission in January 2012, initiating a lengthy legislative negotiation process between the European Parliament and the Council of the EU. After adoption, the general regulation data protection provided for a transitional period of two years. It became fully applicable on 25 May 2018, when the Data Protection Directive was repealed.

2.1 General Data Protection Regulation (GDPR)

The GDPR defines personal data as any information about an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, with particular reference to an identifier such as a name, an identification number, location data, an online identifier or one or more elements characteristic of his physical, physiological, genetic, mental, economic, cultural or social identity. Online identifiers, such as IP addresses, are now considered personal data, unless they are anonymous (Voigt & Von dem Bussche, 2017).

The purpose of the GDPR is in its essence to strengthen personal privacy in the digital age. By protecting the way in which users' personal data can be collected and managed, legislation should give people back control over their dates. It is the General Data Protection Regulation (GDPR), an EU law that controls how companies and other organizations manage personal data. This is the most significant data protection initiative of the last 20 years, with significant implications for any organization in the world that targets EU stakeholders. Function of GDPR is illustrated in Figure 1.

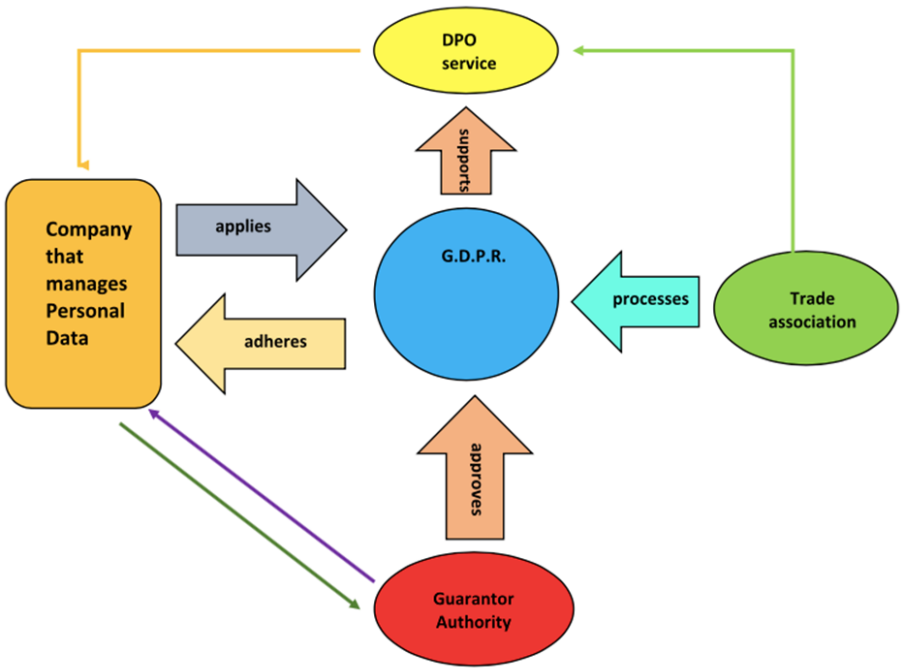

Figure 1. Function of GDPR in relation with companies and trade associations

In order to provide subjects with control over how data is used and to "protect the fundamental rights and freedoms of natural persons", legislation lays down strict requirements regarding data management procedures,

transparency, documentation and user consent. As the data controller, each organization must keep a register and monitor its personal data processing activities. This category includes personal data managed within the organization, but also by third parties, i.e. so-called data controllers.

Data controllers may include software-level service providers as well as integrated third-party visitor tracking and profiling services on the organization's website. Both data controllers and data processors must be able to demonstrate which data is being processed, the purpose of the processing and to which countries and third parties the data is being transmitted. The data may only be transferred to other organizations that comply with the GDPR regulations, or within jurisdictions deemed appropriate. All consents must be recorded as proof that consent has been given. Processing of personal data is not permitted without prior consent. This means that consent must be given before any processing takes place, based on clear and specific information about the type of data and the purposes for which it was collected. For sensitive personal data, consent must be explicit, which underlines the importance of consent when processing sensitive personal data. Individuals now have the "right to data portability" and the "right to access data", as well as the "right to be forgotten", and can withdraw their consent at any time. In this case, the controller must delete the personal data of the natural person if they are no longer necessary for the purpose for which they were collected. In case of a data breach, the company must be able to notify the data protection authorities and the natural persons concerned within 72 hours.

In addition, the GDPR imposes an obligation on public authorities or companies that process sensitive personal data on a large scale to employ or train a data protection officer. The GDPR then introduces a new figure into the world of work, the Data Protection Officer (DPO), who must take measures to ensure that the organization complies with the GDPR. The DPO is an expert consultant with particular expertise in IT, legal, risk assessment and process analysis. This supports the owner in the management of issues relating to the processing of personal data, thus ensuring that a qualified person deals exclusively with the subject of the protection of personal data, updating on the risks and security measures, in view of the growing importance and complexity of the sector.

The role of the DPO is to protect personal data, not the interests of the data controller. This is particularly obvious in the context of public bodies and companies that monitor individuals on a large scale. The DPO must, in fact, possess adequate knowledge of the rules and practices for the management of personal data, and must perform its functions in full autonomy and independence, and in the absence of conflicts of interest. In this sense, a person who is at the top of the company, and therefore able to influence the choices made with regard to the processing of data, cannot hold this position. Obviously, the owner and manager must provide the DPO with the human and financial resources to carry out its task. The role of DPO may be entrusted to one of the company's employees, but it may also be outsourced to a service provider (freelancer or company) by means of a special contract, in which case he/she must also be appointed as data controller. Following is a list of some key points of the directive:

- Increased Territorial Scope : probably the greatest improvement in the regulatory environment of data privacy comes with the increased scope of the GDPR, as it extends to all businesses that handle the personal data of data subjects residing in the Union, irrespective of the location of the business. Originally, the Directive's regional applicability was vague, referring to the information system "in an institution sense". In a number of high-profile court cases, this question has emerged. GDPR makes its applicability very plain - it relates to the collection of personal data by EU controllers and processors, regardless of whether or not the processing takes place in the EU.
- Penalties: all organizations that do not comply with the GDPR may incur penalties ranging from 4% of total annual turnover or € 20 million (whichever is higher), which is the maximum possible tax that can be established. There are specific rules that must be respected. In case of violation of the same there are more levels of sanctions depending on the infringement committed (example: not having the customer's permission for the processing of data or violating the core of privacy). It is important to note that these rules are applied to both controllers and processors, which means that this application also extends to cloud.

- Consent: the conditions for approval have been improved and businesses are no longer able to use terms and conditions that are previously illegible. Consent must be transparent and distinguishable from other matters and in an intelligible and easily accessible manner, using plain language. Withdrawing consent must be simple.

In the context of the Italian legal system, the problem of the protection of personal data arose from the proceedings initiated by the heirs of Enrico Caruso (famous tenor). They asked the judge to block a film because it was considered detrimental to the confidentiality of the tenor. After this there were a number of other proceedings dealing with issues relating to the protection of personal data, but there was no specific jurisdiction. The Italian Constitutional Charter did not provide for the right to the protection of personal data, even though appropriate interpretations were found in Articles 14, 15 and 21, respectively concerning domicile, freedom and secrecy of correspondence, and freedom of expression of thought (Guarda, 2008). The first and most important reference is in Article 2 of the Constitution, where privacy is incorporated among the inviolable rights of man. Italy came as the penultimate in Europe to approve a law for the protection of privacy of general application, first transferred in law 675 of 1996, and then in the Code on the protection of personal data (Privacy Code) that is the Legislative Decree of 30 June 2003, n. 196, which provides the right not to see their data processed without consent, but also the adoption of technical and organizational precautions that everyone must respect in order to proceed correctly to the processing of data of others.

The Code regulates the processing of personal data, including those held abroad, carried out by any person established in the Italian territory or in a State not belonging to the European Union but employing processing tools located in the Italian territory. The Code was amended by a special legislative decree, approved on 8 August 2018, in order to adapt the Italian legislation to the European regulation on the protection of personal data (GDPR). The decree adapts the Code mainly with regard to particularly complex and delicate treatments (e.g. health data), giving the supervisory authority also powers to establish specific safety measures, with the adaptation, the guarantor will have new powers, including the task of introducing simplification for the fulfilment of the obligations of controllers, with regard to small and medium-sized enterprises. A particularly interesting measure that the Supervisor should take in the future concerns the identification of simplified ways of fulfilling the obligations of those holders that can be classified as SMEs. In this regard, it should be reiterated that the Supervisor's possibilities are extremely limited, since such simplified modalities can only be provided within the limits of what is allowed by the GDPR, which provides for very limited derogations for SMEs (for example, as regards record-keeping and certification mechanisms).

It's also important to clarify that the Supervisor's measure will apply only to those companies that meet all the requirements of the SME definition set at European level (less than 250 employees; annual turnover not exceeding EUR 50 million or annual balance sheet total not exceeding EUR 43 million), to be evaluated also taking into account the data of any associated and related companies (Eurostat, 2019). Ultimately, this measure could be far less than expected by many companies that are still struggling to comply with the GDPR. The GDPR's goal is to protect all EU citizens in today's information-driven environment from privacy and data breaches. Although the core principles of data protection remain true to the previous guideline, numerous amendments to the regulatory policies have been proposed. Italy, being part of the European Union, as mentioned above, does not differ much from the EU in terms of the processing of personal data, except with simple changes made by the legislator.

3. Different ways to steal and protect data

This section discusses various ways data theft happens and how they can be protected. Figure 2 illustrates a scheme that describes the process of personal data of physical person and how data is transmitted and protected.

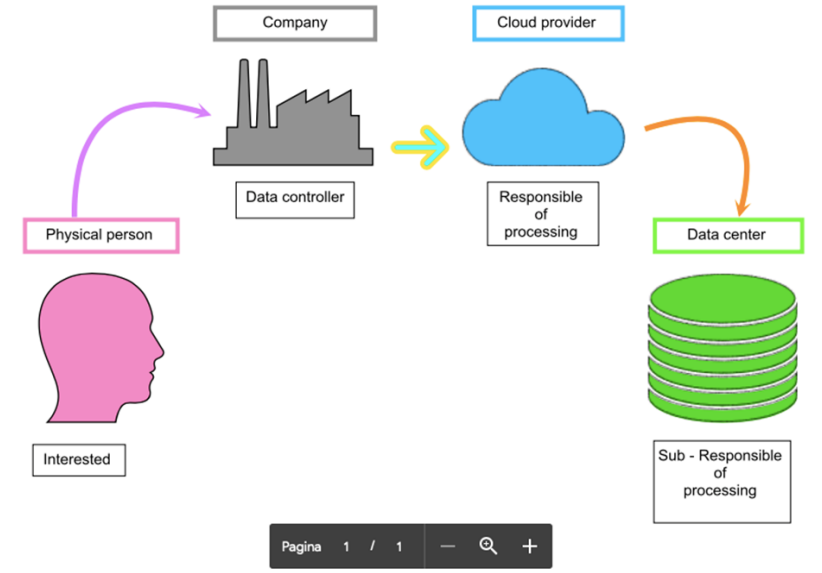

Figure 2. Data transmission and protection process

3.1 Phishing

Phishing and the appearance of Trojan viruses (they are used to steal data but are often associated with other viruses to break down the security of a device) that try to steal information that can be used for shady purposes. Phishing is an illegal activity that exploits a social engineering technique (study of the individual behavior of a person in order to steal information), and is used to obtain access to personal or confidential information for the purpose of identity theft through the use of electronic communications, especially fake e-mails or instant messages, but also telephone contacts (Dhamija, Tygar & Hearst, 2006). Thanks to these messages, the user is deceived and led to reveal personal data, such as bank account number, credit card number, identification codes.

Methodology of attack

The standard process of broaching attack methodologies can summarized in the following steps: the malicious user (phisher) sends the unfortunate and unsuspecting user an email message that simulates, in graphics and content, that of an institution known to the recipient (for example, bank, web provider, an online auction site). The email almost always contains warnings of particular situations or problems that have occurred with the current account / account (such as a huge debit, account expiration, etc.). The email invites the recipient to follow a link, present in the message, to avoid the debit and / or to regularize its position with the institution or company whose message simulates the graphics and setting. The link provided, however, does not actually lead to the official website, but to a fictitious copy apparently similar to the official site, located on a server controlled by the phisher, in order to request and obtain from the recipient particular personal data, usually with the excuse of a confirmation or the need to make an authentication to the system. This information is stored by the server managed by the phisher and then end up in the hands of the attacker. The phisher uses this data to purchase assets, transfer sums of money or even just as a "bridge" for further attacks.

Phishing Defense

Banks, institutions or internet providers never request personal data by e-mail. In the event of a request for personal data, account numbers, passwords or credit cards, it is a good idea, before deleting, to forward a copy to

the competent authorities and notify the bank or other interested parties, so that they can take further action against the false site and inform its users. For any communications, the subjects mentioned above may use an institutional account accessible only from their site, but not the personal email of the citizen. A frequent concern of users who suffer the spillage is to understand how did the attacker knew that they have an account at the bank or online service indicated in the bait message. Normally, the phisher does not know if the victim has an account at the service targeted by the action: the phisher simply sends the same message to a very large number of email addresses, doing spamming, in the hope of reaching by chance some user who actually has an account at the service mentioned. Therefore, no defensive action is necessary apart from the recognition and deletion of the email containing the attempted spillage.

3.2 Pharming

Pharming is a cracking technique used to gain access to personal and confidential information for various purposes. Thanks to this technique, the user is deceived and led to unknowingly reveal to strangers their sensitive data, such as bank account number, username, password, credit card number etc. The ultimate goal of pharming is the same as phishing, i.e. directing a victim to a web server "clone" specially equipped to steal the victim's personal data (Kamal, 2018).

Every time a user types in their browser the address of a web page in alphanumeric form (such as www.alibaba.com) this is automatically translated by computers into a numeric IP address that serves the IP protocol to find in the Internet the path to reach the web server corresponding to that domain. In this sense, for example, by typing the URL “it.wikipedia.org” this is translated by DNS server into an IP address in the format “145.97.39.155”. The DNS name specifies the protocol that regulates the operation of the service, the programs that implement it, the servers on which they run, the set of these servers that cooperate to provide the smartest service.

Pharming Attack

The malicious user operates, with the help of trojan programs or through other direct access, a variation in the victim's personal computer. For example, in systems based on the Windows operating system, by modifying the file "hosts" in the directory. Here, one can enter or change the combinations between the domain concerned (e.g. paypal.com) and the IP address corresponding to that domain. In this way, the victim who has the hosts file modified, while typing the correct URL address in his browser, will be redirected to a server specially designed to steal the information.

Another method is to modify the default DNS servers directly in the registry. In this way the user, without realizing it, will no longer use the DNS of his Internet Service Provider, but those of the cracker, where some combinations between domain and IP address will have been altered. To defend against pharming there are still no specific programs except firewalls (it is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules) that try to prevent access to PC by external users and antivirus programs that block the execution of malicious code. If the site is secure site, a digital certificate issued by a known certification authority will be shown, showing the exact data of the site. This certificate should at least be read and not hastily accepted. In some cases the secure site does not appear as such only because the bank uses a technique of encapsulation of the pages to frames that does not show the padlock in the appropriate box of the browser nor the address in https mode.

So, a first check to defend against spillage sites, is to display the icon, shaped like a padlock in all browsers, which indicates that a secure connection has been established (e.g. SSL – Secure Sockets Layer are cryptographic presentation protocols used in the field of telecommunication and information technology that allow secure communication from source to recipient over TCP/IP networks, i.e. internet). This connection guarantees the confidentiality of the data, while the integrity of the data and the authentication of the counterpart only occur in the presence of the digital signature, which is optional and not reported.

However, an SSL connection could be established with untruthful certificates, through a pair of valid public and private keys, known to those who want to do phishing, but which are not the actual ones of the site. For example, the certificate states that the site "it.wikipedia.org" uses a public key, which is actually that of the phisher. Browsers rather than the user concerned should connect to the site of a certification authority to check: the database shows the public keys and an identifier of the owner, such as the IP address or the site address. Some sites have a specific anti-phishing bar that checks the authenticity of each page downloaded from the site by the means of a digital signature.

3.3 Anti-spillage

There are also specific programs such as the anti-spill bar of Netcraft (is an internet network monitoring company based in Bath, England) and also blacklists that work as a control of access to a certain resource, usable by all, except the entities identified in the list and they allow to alert when the user visit a site probably not authentic. Users of Microsoft Outlook or Outlook Express can also protect themselves through the free Delphish program, a toolbar inserted in MS Outlook or MS Outlook Express with which one can find suspicious links in an email. These programs and the most common browsers do not make use of whitelists (denies a priori to all users the use of the service, except those who are included in the list) containing logical and IP addresses of the authentication pages of all credit institutions.

The spread of e-commerce has coincided with the spread of more and more insidious scams that mainly affect buyers. The main cases are:

- Sale of products from sites owl: Upon receipt of payment goods are not sent, or the shipment is only simulated. The problem is also present on Ebay
- Creation of cloned sites for the purpose of stealing information such as credit card numbers
- Bankrupt companies that accumulate orders, and income, without the ability to process them

Italian law requires that all e-commerce sites report on the home page the VAT number and the name of the company. The most important e-commerce sites have a digital certificate that allows you to verify the authenticity of the site visited. The main problem from the point of view of companies is the management of simulated orders, where false or incorrect details are given for sending products. To reduce the problem many companies only accept advance payments.

3.4 Keylogging

Another spilling technique is the insertion of keylogging applications. In this case, the links may refer to the original site, not necessarily to an imitation. A keylogger is a tool that can intercept everything a user types on the computer keyboard. There are various types of keyloggers including:

- hardware: they are connected to the communication cable between the keyboard and the computer or inside the keyboard
- software: programs that control and save the sequence of keys that is typed by a user.

Hardware keyloggers are very effective because their installation is very simple and the system is not able to notice their presence. Software keyloggers are simple programs that stay running by picking up every key that is typed and then, in some cases, transmit that information to a remote computer. Often these are transported and installed in the computer by worms or trojans received via the Internet and generally have the purpose of intercepting passwords and numbers of credit cards and send them by e-mail to the creator of the same.

Furthermore, Keylogging program can overlap between the browser and the Internet world. In this case, it intercepts passwords. The password is captured independently from the input device (keyboard, mouse, microphone): whether the user types it from the keyboard, or whether it is saved in a text file before connecting to the Internet. Even in the case of a secure (encrypted) connection, if there is a keylogger on the computer that sends the passwords remotely, these passwords can be used by the person who receives them.

4. Conclusions

Despite the tangible benefits that e-commerce has generated over time, many consumers are still averse to the use of digital platforms, especially among the higher age groups. Fears of privacy violations or unlawful acquisitions of personal data by individuals or companies are a fundamental limitation on the spread and growth of digital markets.

Electronic commerce has greatly improved the efficiency of transactions of products and services between sellers and consumers, while at the same time generating considerable cost and time savings. Despite this, the expansion of the digital market has not reached the highest expected levels. A significant proportion of consumers are still linked to traditional market methods (physical transactions). One in three consumers falsifies online data in order to avoid sharing personal information with businesses. It is also a fact that for laziness or to save time users often do not read what they are about to subscribe, online and offline, whether it is a newsletter, a form for a health service or the subscription to an e-commerce service. People could, in fact, avoid receiving unwanted emails or advertisements by simply reading the checkboxes/terms. An incorrect selection of checkboxes is not an irreversible operation, in fact the right to rethink must be guaranteed. Corporate marketing no longer needs personal data. To know the preferences of consumers you do not need the name or the address of the individual, just for example observe posts and movements made on social networks. Sensitive data, therefore, have progressively become less and less important for advertising purposes. Guarantor authorities are working together to improve and modernize the Privacy Directive so that companies also make less invasive use of social media at the expense of users. Further progress can only be made through greater and more solid cooperation between companies and authorities in order to ensure greater protection of consumers' rights and needs in the field of the diffusion of personal data and the protection of privacy.

References

Azmi, I. M. (2002). E-commerce and privacy issues: an analysis of the personal data protection bill. International Review of Law, Computers & Technology, 16(3), 317-330.

Business Insider. (2019). https://www.businessinsider.com/

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 581-590).

European Union. (2019). https://fra.europa.eu/en

Eurostat. (2019). https://ec.europa.eu/eurostat

Guarda, P. (2008). Data Protection, Information Privacy, and Security Measures: an essay on the European and the Italian Legal Frameworks. Information Privacy, and Security Measures: An Essay on the European and the Italian Legal Frameworks (December 2, 2009). Ciberspazio e diritto, 65-92.

Kamal, B. A. (2018). Analysis of increasing hacking and cracking techniques. Scientific and practical cyber security journal.

Kuner, C. (2012). The European Commission's proposed data protection regulation: A copernican revolution in European data protection law. Bloomberg BNA Privacy and Security Law Report (2012) February, 6(2012), 1-15.

Lynskey, O. (2015). The foundations of EU data protection law. Oxford University Press.

Orofino, M., Pizzetti, F. G., Musselli, L., Rosa, F., Ziccardi, G., Ferraro, E., & Zanella, F. (2018). Privacy, minori e cyberbullismo. G Giappichelli Editore.

Pizzetti, F. (2017). Privacy e il diritto europeo alla protezione dei dati personali: Il Regolamento europeu 2016/679. Vol. II. Torino: Giappichelli Editore.

Treccani. (2019). http://www.treccani.it/

Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing.