ISSN 2236-0859

DIREITO & DESENVOLVIMENTO

REVISTA DO PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO E DESENVOLVIMENTO SUSTENTÁVEL

HOW CAN NUDGING SOLVE SOME OF THE INTERNET DATA PRIVACY ISSUES

CINTHIA OBLADEN DE ALMENDRA FREITAS
GIOVANNA MICHELATO ALMADA

VOLUME 10 | NÚMERO 2 | JUL/DEZ 2019

HOW CAN NUDGING SOLVE SOME OF THE INTERNET DATA PRIVACY ISSUES

COMO EMPURRÕES PODEM SOLUCIONAR ALGUNS DOS PROBLEMAS DA PRIVACIDADE DE DADOS NA INTERNET

Received: 12/06/2019
Approved: 15/12/2019

Cinthia Obladen de Almendra Freitas[1]
Giovanna Michelato Almada[2]

ABSTRACT:

The development of new technologies often arouses discussions concerning privacy rights. Consequently, when the Internet became popular and worldwide spread, user privacy concerns also began to arise. Therefore, with the emergence of the information society, the notion of user privacy became variable and has changed over time and according to the region. Consequently, its concept has been modified over the decades too. In 1890, privacy was defined as the right to be left alone. As time passed, the idea of privacy has changed and has become more and more multifaceted, as a reflection of intrinsic aspects of the society. Even with the volatility of this concept, privacy is a fundamental right, as well as essential for a citizen to use the Internet properly. Although it is a fundamental right, people tend to give up on their privacy because of functionalities on the Internet or exchange it for small rewards. However, users often do not have the knowledge about the exchanges or violations. In order to solve some of the Internet data privacy issues, Libertarian Paternalism may be used. Different researches were conducted by applying this theory in the data privacy sphere. By using *nudges*, it is possible to help people choose wisely how to protect privacy, or at least to give them the right amount of information and guide users to the best option.

Keywords: Privacy. Behavioral Economics. Libertarian Paternalism. Information Society. Information and Communication Technology.

RESUMO:

O desenvolvimento de novas tecnologias desperta frequentemente discussões sobre direitos de privacidade. Consequentemente, quando a Internet se tornou popular e disseminada em todo o mundo, preocupações com a privacidade do usuário também começaram a surgir. Portanto, com o surgimento da sociedade da informação, a noção de privacidade do usuário se tornou variável e mudou ao longo do tempo e o espaço. O conceito de privacidade vem sendo modificado ao longo das décadas. Em 1890, a privacidade foi definida como o direito de ser deixado em paz. Com o passar do tempo, a ideia de privacidade mudou e tornou-se cada vez mais multifacetada, como um reflexo de aspectos intrínsecos da sociedade. Mesmo com a volatilidade desse conceito, a privacidade é um direito fundamental, além de essencial para cidadãos usarem a Internet de

1 Possui graduação em Engenharia Civil pela Universidade Federal do Paraná, mestrado em Engenharia Elétrica e Informática Industrial pela Universidade Tecnológica Federal do Paraná e doutorado em Informática pela Pontifícia Universidade Católica do Paraná. É Professora Titular da Pontifícia Universidade Católica do Paraná - PUCPR para os cursos de Direito (Direito Eletrônico; Direito e Informática; Propriedade Intelectual; Perícias e Laudos Técnicos; Fraudes e Crimes por Computador). Professora Permanente do Programa de Pós-Graduação (Mestrado/Doutorado) em Direito (PPGD). Email: cinthia@ppgia.pucpr.br
2 Mestranda em Direito pela Pontifícia Universidade Católica do Paraná. Advogada. Email: gmichelato@gmail.com

maneira adequada. Embora seja um direito fundamental, as pessoas tendem a abrir mão de sua privacidade por causa de funcionalidades na Internet ou trocá-la por pequenas recompensas. No entanto, os usuários geralmente não têm conhecimento sobre as trocas ou violações. A fim de resolver alguns dos problemas de privacidade de dados na Internet, o Paternalismo Libertário pode ser aplicado, visto que diferentes pesquisas foram realizadas aplicando essa teoria na esfera da privacidade de dados. Usando *nudges* (empurrões), é possível ajudar as pessoas a escolher sabiamente como proteger a privacidade ou, pelo menos, dar a elas a quantidade certa de informações e orientar os usuários sobre a melhor opção.

Palavras-chave: Privacidade. Economia Comportamental. Paternalismo Libertário. Sociedade da Informação.

Classificação Journal of Economic Literature (JEL): K10, K39 (Law and Technology).

1. INTRODUCTION

Human beings are creative, inventive, social beings, but not perfect. Because of this lack of perfectness, people tend to choose wrongly, even when trying to protect their interests. As a matter of fact, even when they are well informed, people tend to fail on achieving their preferred purposes for many reasons. This kind of inability happens in different fields of choice, even when protecting fundamental rights such as the right to privacy.

Behaviour sciences, for the past decades, try to understand how the human decision-making process is bounded by (ir)rational and systematic biases. Thaler and Sunstein understand that bad behavioural choices of humans are the reflection of cognitive limitations, biases, or habits (THALER; SUNSTEIN, 2009). As a solution for this flaw, the authors suggest that people must be *nudged* toward the best option – that would be the option that best fulfils one's interests.

The concept of *nudge* came from behavioural science and was reflected in different fields, such as political science, psychology and economics. In overview, Thaler and Sunstein define a *nudge* as:

> (...) any aspect of the choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not. (THALER; SUNSTEIN, 2009, p. 6).

Nudges, therefore, are an indirect suggestion that would positively influence people's decision-making. Therefore, they are tools that should be used to provide more effective public policies, reducing governmental costs that a wrong choice may create (IGLESIAS, 2017).

The *nudge* theory has a crucial point that is directly related with privacy choices: most of the time, people tend to stick to what is offered as default, without investigating or even changing it to an option that would better fit their interests. One example is when installing new software, or even signing up for a new social network, people use the 'recommended' configurations, without thinking of what it means. People do not investigate what the 'recommended' configurations are, or which 'privacy policy' the website/software is using. They stick with the default.

In this perspective, a new phenomenon emerges, the 'interpersonal privacy concerns', which are the perceptions, interactions and behaviours that are not congruent with the real world.

> While individuals are free to decide what personal information they disclose, they often cannot control what others disclose about them, or how others may use the private information that they disclose. Likewise, people may share information that involves others in ways that violate their privacy preferences. This becomes an increasingly significant privacy threat with the emergence of SNSs [social network sites], as the digitized social platform combines an individual's self-disclosure with others' disclosure of information about the individual, records the information in rather permanent fashion, and often presents the information publicly, making it accessible to and beyond one's social circles (JIA; XU, 2015, p. 1).

Taking into consideration that privacy is the fundamental right for a citizen to enjoy the network potential (DONEDA, 2014; FORTES, 2016), behavioural science and the *nudges* can be an answer to some of the current privacy concerns that are being raised nowadays. To prove that, the present article will address: (i) how the personal data-privacy concept has evolved over the years; (ii) why the users cannot manage privacy; (iii) how the Libertarian Paternalism can satisfactorily address this matter.

So, knowing that although people have concerns about privacy, and also understanding that privacy must be protected, why do people tend to give up on this right in order to use the Internet? In order to address this question, the present article uses inductive reasoning, starting with the observation of theories involving behavioural economics and user data privacy, using indirect documentation, through bibliographic research. This allows us to draw a line between the concern regarding privacy and the *nudges* from the behaviour economics. And it is possible to draw a line between both areas, by understanding the premises.

Since behaviour economics addresses how people can be nudged towards a certain act or behaviour, this article tries to understand how this could be applied in the field of user privacy, in order to protect the user from possible threats. Another point that will be raised is related to the problem with the self-management of privacy by the users, once they are not fully aware of the problem and also do not have the technical knowledge.

2. THE RESHAPED PERSPECTIVE OF DATA PRIVACY IN THE INTERNET

The discussion regarding the right to privacy is a consequence of the rise of new technics and technological instruments, since it may facilitate the access and, therefore, the disclosure of facts and information that were not showed to the public (DONEDA, 2014). This idea was first discussed by Warren and Brandeis, in 1890, when they addressed how photography, newspapers and other technological appliances had invaded the sacred realms of private, domestic life.

In this particular article, the authors brought the concept that privacy is the right "to be left alone" (WARREN, BRANDEIS, p. 195). Therefore, the right to privacy becomes directly related with the inviolability of personality protection, breaking the previous idea and linking with the protection of private property. However, the idea of privacy is not very accurate, being a reflex of the society and the relevant period of time (DI FELLICE; LEMOS, 2014).

Over time, the idea of privacy and, consequently, its protection has changed. In the 20th century, the change of the role of the States, aligned with technological revolution made the concept of right to privacy to change and spread. What was a right of a strictly

negative conception – since privacy was seen as if it was hiding something terrible – became a guarantee of individual control of their information, an assumption of any democratic regime (DONEDA, 2014). Therefore, this right acquired a positive conception and became a recognised international right – and matter of discussion (RODOTÀ, 2008).

In the 1970s, the discussion regarding privacy started to arise globally. Different legislations started regulating the right to privacy around the world, judicial decisions started to emerge, and an international Treaty was discussed among countries. In that specific time, the conception of privacy was that it was a projection of the individual personality and, therefore, legal protection was needed.

The first generation of data privacy regulations emerged as an answer to the electronic processing of data in governments and private companies. Also, at that moment there was a tendency of the creation of centralised databases in a unique database, management by national governments (AGREL; ROTENBERG, 1998).

The United States Government, in 1965, proposed the creation of a *National Data Center*, to manage the national budget and reduce costs (GARFINKEL, 2000). The idea was to create a unique data center that would eliminate the investments of other agencies in computer centers and data storage. However, this project was never materialised, since people started to fear the 'power' that the government would have because of this *National Center*. It would inflict directly on the American tradition of liberalism (DONEDA, 2006).

When technology allowed the storage and processing of data, a link between privacy and personal data protection was formed. The right to privacy started to change, as well as how it was presented. The expressions 'information privacy', 'personal data protection', 'information self-determination', etc., are now used to address this matter.

The second generation of data privacy regulations emerged from the necessity of changing the existing legislations. These legislations sought to expressly address the right to privacy and not only regarding data processing. The fear of a unified database was replaced by a fear of different databases spread worldwide, connected to each other and managed by public agencies and private companies. In this context, the right to privacy became regimented not only by ordinary law but also became a constitutional right. An example of this new legal approach is the existence of laws from Austria, France, Denmark and Norway.

However, the second generation of laws brought up a new controversial issue, related to the effectiveness of citizens' consent and if there is a real exercise of the consumer freedom of choice, knowing that if a person refuses to provide his/her data, it may cause his/her social exclusion.

This fact brings the third generation of data protection laws, marked by the decision of the Federal Constitutional Court of Germany, which interpreted the German Federal Data Protection Law in consonance with the Fundamental Law of Bonn. The Court understood that all citizens had the right to the auto-determination of information, with the idea of users controlling their data (MARTINS, 2005).

The main difference between the second and third generations is related to the participation of the citizens in the data processing. In the third generation laws, the user takes part in the whole process, from the data collection to the data storage and sharing (MENDES, 2014).

In its turn, the fourth generation of normative laws tried to solve the problems regarding consent and remedies to data leaking (VIOLA DE AZEVEDO CUNHA, 2010; BOTTA; 2010). Firstly, these laws aimed at making the users position stronger, making possible their effective auto-control over their data. As an example of this approach, there is the *no-fault compensation*

that addresses individual personal complains regarding data violation in Germany or Norway (MAYER-SCHÖNBERGER, 2001).

Secondly, it removed some data from the individual control, since the content of this particular data is so essential that must be extremely protected. Therefore, it could not be available at the disposal of an individual (SIMITIS, 1999). This type of treatment can be seen regarding '*sensible data*', that is, every data whose disclosure can result in private discrimination, such as information regarding sexuality, ethnicity, political opinions, religion, etc.

The data protection matter emerges in the information society as an alternative to protect the individual personality, against risks aroused with data processing (PARISER, 2012). The goal is to protect the person who owns the data and not the data itself.

As pointed out, the discovery of new technologies made data collection, data logging, data crossing, data organisation and data transmission possible, in a scenario that was never imagined. This technology has made it possible to gather valuable information of citizens, facilitating economic, political and social decision-making (ALCALÁ, 2005). The value of information is not only a matter of data storage capability but mainly by the possibility of 'creating' new information from data processing. In other words, the processing of previously stored data creates new information, without the need of a new collection. New data is created from existing data, regardless of its collection being directly from the user (DE LA CUEVA, 1999). One example is the *profiling* techniques, which are used to predict the decision-making of the consumers, workers and citizens in general – it can influence the consumption of people's choices.

In this scenario, there is a *tradeoff* between technology and privacy, since the enlargement of technology reduces personal privacy. Consequently, one may think that the only solution to restrain it is to prevent the development of information technologies. However, the most effective way of perusing this problem was pointed out by Simson Garfinkel. According to the author, the matter should be answered by the conception that the technological development must be sought concomitantly with the preservation of citizens privacy (GARFINKEL, 2000).

The way the Internet is organised makes users feel obliged to provide information, or even to do it without the full awareness regarding this act. Therefore, the 'solution' pointed out by Garfinkel is only possible if the users have the chance to preserve their privacy. However, unfortunately, consumers do not choose good options in general.

3. THE PROBLEM WITH PRIVACY SELF-MANAGEMENT

Although data privacy is a matter of concern for Internet users, there are many inconsistencies and contradictions regarding the way it is addressed. On the one hand, people feel entitled to protect personal and sensible information. On the other hand, users end up trading away some information for small rewards.

There is a simple and practical example for that. Usually, when a person needs to use an online service, social network, website, or even do a flight check-in, for example, he/she will need to sign in to this particular service. To do that, several fields will be required to be filled in, with information such as name, surname, date of birth, email, address, etc. As a way to facilitate the process, some websites offer a 'simplified' sign up, using the social network – mostly your Facebook account.

As previously pointed out, there were many scandals related to Facebook data leaking, such as Cambridge Analytica (LAPOWSKY, 2018; CONFESSORE, 2018; OSBORNE, 2018). However, the user keeps using this sign-up 'tool', as a form of saving time in the entering of

information. Most of the time, people do not even realise which information is being shared or even to whom. Moreover, these scandals are not restricted to social media, but also in an international sphere, regarding governmental surveillance (BOLZAN; NETO, 2014), such as those leaked by Wikileaks and Edward Snowden.

For Acquisti (2009), many social scientists had the assumption that people have decided on a particular preference for privacy and based in that preference started making coherent *tradeoffs* between privacy and other goals. However, this rationale is inaccurate, since humans are not as accurate as we presume, nor make good choices as it is expected.

Behaviour decision search and behavioural economics literature have found out systematic incongruences in consumer choices. Preferences, in general, are often liable and influenced by contextual factors. People create preferences based on how alternatives are framed, or even on how information is presented to the users – if any information is available. Also, choices will be made according to the comparisons they evoke, and according to the background of that particular individual with those alternatives.

It is important to notice that opt-in and opt-out are explicit consumer data collection architectures (SCOTT, 2013). In an opt-in program, a user must take action to have his/her data included in a list or database. An opt-in is essential if the user intends to be added to any kind of emailing list. Opting in usually occurs when someone signs up for a series of emails, such as an e-newsletter or coupons for specific products. An opting out program forces users to take an action in order to be removed from the advertisers' lists or databases used to target advertisements to the individual user tastes. By default the user data is included in a list or database. This architecture causes privacy violation because brands, consumers, and third parties are more likely to suffer, should websites and tech platforms become subject to opt-in architectures. Systems that are not reliable or based on misunderstanding may reduce the number of potential users, which reduces the availability of user data. A reduced user data makes it more difficult for the business to offer broad, personalized services, which in turn leads to less use by advertisers. The opt-in consumer data collection architecture has been the path taken by current legislations on the protection of personal data. And, "the browser-level opt-in must be combined with legislative efforts to make data collection, retention, and disclosure practices more transparent" (SCOTT, 2013, p. 287).

Privacy consequences are not easily estimated or cannot be easily seen in advance by the users. The main reason for that is that many effects can influence and even distort the way it is valued. Therefore, the concern or the value of data protection is postponed and even distorted by the consumer. In most of the cases, the users start caring about it, after this right is violated and the data has been leaked out – and once it happens, it would be very hard to constrain or reverse the leaking.

Privacy decisions often involve the balance between control over what is shared and the costs and benefits of sharing or hiding some personal information. These *trade-offs* became a subject of study of a field of economy, denominated 'privacy economics'. Privacy economics deals with these trade-offs, by trying to "understand, and sometimes quantify, the costs and benefits the data subjects (as well as potential data holders) bear or enjoy when their personal information is either protected or shared" (ACQUISTI, 2009). Also, it tries to understand "how to use market mechanisms, technology or policy to achieve a desirable balance between information revelation and protection, with the satisfaction shared among the individuals, organizations, and society" (ACQUISTI, 2009, p. 72).

In 2004, Acquisti started a research that consisted on the application of theories and methodologies from behavioural economics and behaviour decision to understand de privacy decision-making matter. He focused on the cognitive and behavioural biases, from risk

aversion to immediate gratification. In his research, he found out the need for "more substantial theories to understand how challenges and hurdles affect the way we make decisions about our personal information". These difficulties, for instance, may come from several factors such as: "inconsistent preferences and frames of judgment"; "information about risks, consequences, or solutions inherent to provisioning (or protecting) personal information"; "bounded cognitive abilities that limit our ability to consider or reflect on the consequences of privacy-relevant actions", etc. (ACQUISTI, 2014)

The rational choice theory defends that people will maximise their utility over time, making choices based on their previous experiences and, therefore, minimizing the chance of errors. However, humans are known for making bad decisions – and this fact is reflected in the privacy field.

The way people tend to make choices regarding privacy are directly affected by incomplete and asymmetrical information. This means that the individual that is the subject of data collection knows less than the data collectors. In other words, the data holders have more knowledge about the magnitude of data collection and how it will be used, and its implications.

The way that Internet is shaped, the way data is collected and used has changed all the way society is built in. This change resulted in many consequences that people cannot understand and, therefore, are not able to consider in their entirety (ACQUISTI, 2008). This lack of 'view' of the whole picture is called *bounded rationality*, since humans often replace rational decision-making methods with simplified mental models and heuristics (THALER, SUNSTEIN, 2009).

However, even if the access to all this information were made possible, the users may not choose the best way possible. Many behavioural anomalies and biases make people chose differently from the predicted by rational choice theory (CAMERER; LOEWENSTEIN, 2002).

Users relying upon incomplete information make privacy choices. Personal control over the information sphere is at least not determinate, or even not imitated (POSNER, 1978). An example given by Acquisti and Grossklags is that information asymmetries "often prevent a subject from knowing when another entity has gained access to or uses their personal information". Consequently, the subject may not have the full knowledge about the potential consequences of the privacy violation.

However, exercising control over the private data in the context of big data is challenging – there is an enormous amount of data being collected every day (INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO DE JANEIRO, 2016). In this context, the user has none or very little control over which data is being collected, stored and shared.

4. NUDGING: THE LIBERTARIAN PATERNALISM SOLUTIONS

As already presented, users have vague and limited information on the actions one can take in order to protect one's data. In the same way, they have a restricted knowledge regarding the actions that data collectors are making in order to hold one's data. Also, the consequences are complicated to predict. One of the reasons is that problems will be only visible in the future, after they occur – and, because of that, some actions are not available yet. However, some individuals ignore privacy risks and the protection actions one can make, even when they are aware of them. This is often miscalculated, making the user choosing wrong.

As an answer to this ambiguities, uncertainties and bad choices, the Libertarian Paternalism can be a solution. Firstly, it could help individuals understand risk and deal with

bounded rationality. Secondly, it can be used in framing and heuristics. Moreover, lastly, in other systematic biases, as it will be shown.

Knowing that users have difficulties on identifying outcomes related to privacy issues, the best form of protection is Libertarian Paternalism, which can help to 'protect' these users. Public policies emerge in order to demand some protection standards. However, it is important to stress out that giving more information does not mean that individuals will be able to process it – and this is more difficult since data privacy information is very complex and specialised.

It is in this context that Libertarian Paternalism presents a solution. In 2005, Acquisti and Grossklags applied a survey regarding individual privacy attitudes and behaviour. They found out that a number of the participants combined security and privacy issues when reported the feeling that their privacy was protected by merchants who offered SLL connections to complete online payments. In the same way, when there was a privacy policy, users felt more secure, regardless of its content. Also, if a website has a security seal, people tend to interpret it as trustworthy (ACQUISTI; GROSSKLAGS, 2005).

Researchers found out that even when information regarding the dangerous behaviour of computer programs are presented, such as spyware, individuals not always abort the installations (GROSSKLAGS, 2007). However, it was found that presenting some additional information may influence the choice-process, making users think twice before deciding.

It is also important to understand that the way the matter is *framed* influences directly how the person responds to it. Acquisti and Grossklags (2005, p. 30) found out that there is a direct impact on the willingness of a person to "accept or reject a marketer's privacy-related offer when the consequences of the offer are re-framed in uncertain and highly ambiguous terms". Hence, the most effective strategy is to convince consumers before they give personal information (ACQUISTI; GROSSKLAGS, 2008, p. 370). A research conducted by Good *et al.* found out that advice given in a vaguer language is considered less intrusive and, therefore, more effective, when advising on this matter (GOOD, 2006).

Several *heuristics* can guide people in the individual decision-making process better than the rational choice process. As shown by Thaler and Sunstein, people tend to *anchor* on a specific valuation of a good or service, and then re-adjust according to new information discovered. Differently from other goods or services, people have difficulties in pricing their information. However, once the individual has found the price "it is likely that the consumer's valuation of their data will hereafter orbit around that value" (ACQUISTI; GROSSKLAGS, 2008, p. 8). When individuals realise that their data has been given, they tend to assign a higher selling price than the buyer value. There is also the fact the individuals often accept small rewards.

The application of *nudges* may enhance the exercise of privacy rights. Several researches made in the United States found that different designs of privacy *nudges* might have a positive impact on how users use online platforms (JIA; XU, 2015).

Iglesias points out one example of nudge, made by Mozilla Foundation. In February 2013, they released a Firefox updated patch for its privacy settings, with the assumption that users would stick with the default option. The default would forbid third parties' cookies to be accepted while browsing the Internet. Knowing that users seems to stick with the default options, this patch increased positively the individual's privacy, since only the websites that were indeed visited will have their cookies allowed.

Cookies[3] are an Internet tracking method applied by the browser during an open session between the browser and the server in HTTP protocol (Hypertext Transfer Protocol) (CASTELLUCCIA, 2012, p. 23). But there are currently many tracking methods on the Internet

3 A cookie is a piece of text stored by a user's web browser and associated to a HTTP request. A cookie consists of one or more name-value pairs containing bits of information and is set by a web server.

that collect data and penetrate user privacy: "[t]he broader the Internet activity becomes, the more intense the involvement of the site owners, as well as third parties who can make money by sharing information collected by them regarding the users" (CARMI; GOLAN; BOUHNIK, 2016, p. 201).

On the other hand, despite the user privacy violation brought by cookies, they grant a lot of advantages to the site developer, the advertiser and the publisher, including the users that have a quick website access. Some of the Internet site operations are not possible without cookies, such as online ordering, Internet site tracking and identification of users. Moreover, tracking users locations and time spent surfing on the site can assist on making changes in order to improve the user experience and modify contents, thus increasing the probability of the user's return. So, ICT companies can provide various techniques and methods for online tracking.

Moreover, there is the possibility of an *Audience Nudge* tool, developed by Carnegie Mellon and Syracuse Universities, in order to allow social network users to consider who is able to see their posts. The tool works in a way that displays five random profile pictures from your friends or followers list, as a reminder of the potential audience for the post (WANG, 2013).

It is important to notice that profiling refers to computational methods and techniques applied to personal data or not collected from Internet users or other systems. And in the Big Data era, there is no absence of data to be collected and processed. Profiling techniques aim to determine what is relevant within a given context. Moreover, these techniques help in statistical representativeness, that is, in determining the quality of a sample constituted to correspond to the population in which it is chosen. That is, it seeks to generalize from a sample of individuals and their respective interests. There are many profiling definitions and some of them are relevant to this paper: "[t]he act or process of extrapolating information about a person based on known traits or tendencies, e.g. consumer profiling" (FERRARIS, et. al., 2013, p. 6). And, "profiling is the act of suspecting or targeting a person on the basis of observed characteristics or behaviour, e.g. racial profiling" (FERRARIS, 2013, p. 6).

Profiling is a process of construction of a series of information (a profile), which is then applied to something or someone (individual or group) by techniques of data elaboration (FERRARIS, 2013, p. 6). The data elaboration mentioned is data collecting and processing by computers and computational systems. Profiling can also be defined as a new way of knowing that makes visible the patterns that are invisible to the human eye.

Syracuse University scholars have also developed another type of *nudge design*, this time to encourage users to reflect on what has been written on networking platforms. The main objective of this *nudge* is to make users reflect about what is being posted, in a way to prevent disproportional outcomes:

> When a user starts typing a status update or comment, a message with a yellow background appears stating, "You will have 10 seconds to cancel after you post the update." After the user clicks the "Post" button, the user is given the option to "Cancel" or "Edit" the post during a ten-second countdown before the post gets published on Facebook. There is also an option to circumvent the timer by clicking a "Post Now" button. (WANG, 2013, p. 1321)

Although this *nudge* had some positives outcomes, some participants ignored the notices after some days.

Another research conducted by Carnegie Mellon University found that people pay more attention to personal data shared by online apps when they are told about it. In other words, people tend to understand the privacy issue, or at least how data is being collected, if it is showed in real time. This study focused on understanding if permission managers are

efficient, when combined with privacy *nudges*. In order to do that, the application *AppOps* released notices about the quantity and the way different third parties received the data. As a result, users found out that the data was shared even more than imagined (SPICE, 2015). http://moritzlaw.osu.edu/students/groups/oslj/files/2013/12/19-Wang-Leon-Chen-Komanduri-Norcie-Scott-Acquisti-Cranor-Sadeh.pdf

All these nudges are practical examples on how Libertarian Paternalism could be used. However, as in other areas where this theory is applicable, there are some questions raised. Cristian Schubert (2016) rises ethical questions of *nudges* that may be applied in the data privacy area too. In the first place, Schubert asks whether *nudges* will increase people's well-being. Secondly, if *nudges* will affect personal *autonomy*. In the third place, he questions if the *nudge* may affect people's integrity. And lastly, if there are practical applications.

These questions must be answered in the most beneficial way possible. The most adequate answers will provide a *nudge* design that could be as effective as possible, considering its positive and negative effects in the long term.

5. CONCLUSION

It is a fact that as the use of technology increases, the problem with privacy will certainly increase too. This matter on Internet does not deal only with the fact that humans do not make good choices. The problem is that users do not have the technical knowledge to solve these problems.

Therefore, the Libertarian Paternalism may be the answer to protect users and help them make good choices. However, there will be questions to be answered, regarding the *nudges*, which are the same questions brought by the Libertarian Paternalism criticism. Who will be the one to consider one privacy policy the 'best' one?

Even with these questions, the use of the *nudges* may improve policy decision making and technology design for end users. Using this economic theory, people would be able to use the Internet, the social networks and other online services without the risk of violating their fundamental right of privacy. With this overview, people will be able to choose if they want to disclosure personal data and have the knowledge on how this information is being shared.

REFERENCES

ACQUISTI, Alessandro; GROSSKLAGS, Jens. Privacy and Rationality in Individual Decision Making. **IEEE Security & Privacy Magazine**, January/February, 2005, p. 24-30. Institute of Electrical and Electronics Engineers (IEEE). Available at: <http://csis.pace.edu/~ctappert/dps/d861-09/team2-3.pdf>. Access on 08 June 2019.

ACQUISTI, Alessandro; GROSSKLAGS, Jens. What Can Behavioral Economics Teach Us about Privacy? In: ACQUISTI, Alessandro et al. **Digital Privacy**: Theory, Technologies and Practices. London: Auerbach Publications, 2008.

ACQUISTI, Alessandro. Nudging Privacy: The Behavioral Economics of Personal Information. **IEEE Security & Privacy Magazine**, [s.l.], v. 7, n. 6, p.72-85, nov. 2009.

ACQUISTI, Alessandro. Privacy in electronic commerce and the economics of immediate gratification. **EC '04 Proceedings of the 5th ACM conference on Electronic commerce**. New York: ACM Press, 2014.

AGREL, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. **Harvard Journal of Law & Technology**, Cambridge, v. 11, n. 3, Summer 1998, p.871-880.

ALCALÁ, Humberto Nogueira. Autodeterminación informativa y hábeas data en Chile e información comparative. **Anuário de Derecho Constitucional Latinoamericano 2005**, t. II, Konrad Adenauer Stiftung.

BOLZAN, José Luiz; NETO, Elias Jacob de Menezes. A Insuficiência do Marco Civil da Internet na Proteção das Comunicações Privadas Armazenadas e do Fluxo de Dados a Partir do Paradigma de Surveillance. In: Leite, George Salomão, Lemos, Ronaldo (Coord.). **Marco Civil da Internet**. Atlas, 09/2014.

BOTTA, Marco; VIOLA, Mario. La protezione dei dati personali nelle relazioni tra UE e USA: le negoziazioni sui trasferimento dei PNR' (2010)**, Diritto dell'informazione e dell'informatica,** Vol. 26, no. 2.

BVefGE 65, 1, Volkszählung. Ver MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Montevidéu: Fundação Konrad Adenauer, 2005.

CAMERER, Colin F.; LOEWENSTEIN, George. **Behavioural Economics**: Past, Present, Future. 2002. Available at: <http://people.hss.caltech.edu/~camerer/ribe239.pdf>. Access on 08 June 2019.

CARMI, Golan; BOUHNIK, Dan. Functional Analysis of Applications for Data Security and for Surfing Privacy Protection in the Internet. **International Journal on Recent and Innovation Trends in Computing and Communication - IJRITCC** , Vol. 4, Issue 7, July 2016,

CASTELLUCCIA, Claude. Behavioural Tracking on the Internet: A Technical Perspective. S. Gutwirth et al. (eds.), **European Data Protection**: In Good Health? – Chapter 2. Springer Science+Business Media B.V., 2012.

CONFESSORE, Nicholas. Cambridge Analytica and Facebook: the scandal and the fallout so far. **The New York Times.** 04 abr. 2018. Available at: <https://nyti.ms/2GBQ4Lm>. Access on 08 June 2019.

DE LA CUEVA, Pablo Lucas Murillo. La construcción del derecho a la autodeterminación informative. **Revista de Estudios Políticos**, Madrid, 104, (Nueva Época), Abril/Junio 1999.

DI FELLICE, Massimo; LEMOS, Ronaldo. **A Vida em Rede**. São Paulo: Paprius, 2014.

DONEDA, Danilo. A proteção da privacidade e de dados pessoais no Brasil. **Observatório Itaú Cultural**: Direito, Tecnologia e Sociedade, Rio de Janeiro, ed. 16, p. 136-149, jan/jun 2014.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

FORTES, Vinicius Borges. **Os direitos de privacidade e a proteção de dados pessoais na Internet**. Rio de Janeiro: Lumen Juris, 2016.

GARFINKEL, Simson. **Database National:** the death of privacy in the 21th century. California: O'Reilly Media, 2000.

GOOD, Nathaniel, et al. **User Choices and Regret: Understanding Users' Decision Process About Consensually Acquired Spyware**. A Journal of Law and Policy for the Information Society, Vol. 2, No. 2, pp. 283-344, 2006. Available at: <https://papers.ssrn.com/abstract=2262437>. Access on 08 June 2019.

GROSSKLAGS, Jens; et. al. Noticing notice: a large-scale experiment on the timing of software license agreements. Proceedings od SIGCHI **Conference on Human Factors in Computing Systems,** 2007. Available at: <http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags07-CHI-noticing_notice.pdf>. Access on 08 June 2019.

IGLESIAS, Daphnee. **Nudging Privacy**: benefits and limits of persuading human behaviour online. Available at: <https://itsrio.org/wp-content/uploads/2017/03/Daphnee-Iglesias-.doc-B.pdf>. Access on 08 June 2019.

INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO DE JANEIRO (ITS RIO). **Big Data no projeto Sul Global**: Relatório sobre estudos de caso. Rio de Janeiro: Its Rio, 2016. Available at: <http://itsrio.org/projects/big-data-in-the-global-south-project-report-on-the-brazilian-case-studies/>. Access on 08 June 2019.

JIA, H. and XU, H. **Interpersonal Privacy Nudges for Promoting Privacy Protective Behaviors on Social Network Sites**. Available at: <http://cs-sys1.uis.georgetown.edu/~sz303/PIR2015/pir_submission/pir2015_submission_5.pdf>. Access on 08 June 2019.

LAPOWSKY, Issie. Facebook exposed 87 million users to Cambridge Analytica. **WIRED**. 04 abr. 2018. Available at: <https://bit.ly/2IUlptC>. Access on 08 June 2019.

MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. **Technology and privacy:** the new landscape. Cambridge: The MIT Press, 2001.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

OSBORNE, Hilary. What is Cambridge Analytica? The firm at the centre of Facebook's data breach. **The Guardian.** 18 mar. 2018. Available at: <https://bit.ly/2prhWXb>. Access on 08 June 2019.

PARISER, Eli. **O filtro invisível**: O que a Internet está escondendo de você. 1. ed. Rio de Janeiro: Zahar, 2012.

POSNER, Richard A. An economic theory of privacy. **Regulation: AEI Journal on Government and Society,** [S.L.], v. 2, n. 4, p.19-26, May/June 1978. Bimonthly. Available at: <https://www.cato.org/pubs/regulation/regv2n3/v2n3>. Access on 08 June 2019.

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Trad. Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCOTT, Erica M. Protecting Consumer Data While Allowing the Web to Develop Self-Sustaining Architecture: Is a Trans-Atlantic Browser-Based Opt-In for Behavioral Tracking the Right Solution? **Global Business & Development Law Journal**, Vol. 26, p. 285-313, 2013.

SCHUBERT, Cristian. A note on the ethics of nudges. VOX, 22 January 2016. Available at: <http://voxeu.org/article/note-ethics-nudges>. Access on 08 June 2019.

SIMITIS, Spiros. **Revisiting sensitive data**: review of the answers to the questionnaire of the consultative committee of the convention for the protection of individuals concerning automatic processing of personal data (ETS 108). Strasbourg, 24-26 November 1999. Available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680684 5af>. Access on 08 June 2019.

SPICE, Byron. Study Shows People Act To Protect Privacy When Told How Often Phone Apps Share Personal Information. CMU News, Carnegie Mellon University, 23 March 2015, p. 3. Available at: <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1335&context=heinzworks>. Access on 08 June 2019.

THALER, Richard H.; SUNSTEIN, Cass R. **Nudge: o empurrão para a escolha certa:** Aprimore suas decisões sobre saúde, riqueza e felicidade. Rio de Janeiro: Elsevier, 2009.

V. Ferraris, et al., **Defining profiling**. United Nations Interregional Crime and Justice Research Institute (UNICRI), [e-book], 2013, www.unicri.it/news/files/Profiling_final_report_2014.pdf (accessed 23 February 2018), p. 6.

VIOLA DE AZEVEDO CUNHA, Mario. Privacy, Security and the Council Framework Decision 2008/977/JHA. **World Jurist Association Law and Technology Journal**, v. 43, p. 1-18, 2010. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1666140>. Access on 08 June 2019.

WANG, Y. *et. al.* From Facebook Regrets to Facebook Privacy Nudges. Heinz College Research, Carnegie Mellon University. **Ohio State Law Journal**, 74, 1307-1335. Available at: <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1335&context=heinzworks>. Access on 08 June 2019.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. IV, n. 5, 1890.