MASTER’S THESIS (DOUBLE DEGREE):

RETHINKING INFORMED CONSENT:
GIVING BACK CONTROL TO THE DATA SUBJECT FROM A BEHAVIORAL ECONOMICS PERSPECTIVE

By:

Santiago Ramirez Lopez

Supervisor:

Dr. Christof Tschohl

Date of submission: August 18, 2016

Deadline for submission: August 29, 2016
I. Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction:</td>
<td>3</td>
</tr>
<tr>
<td>Privacy in Western traditions: A story about finding and losing control:</td>
<td>7</td>
</tr>
<tr>
<td>Privacy as control:</td>
<td>7</td>
</tr>
<tr>
<td>Privacy as control: Outdated or ignored?:</td>
<td>9</td>
</tr>
<tr>
<td>Current state of affairs: An unbalance between regulation and social perception:</td>
<td>12</td>
</tr>
<tr>
<td>Consent:</td>
<td>12</td>
</tr>
<tr>
<td>Other mechanisms of control:</td>
<td>15</td>
</tr>
<tr>
<td>Data protection regime: The unbalance between regulation and social perception:</td>
<td>18</td>
</tr>
<tr>
<td>Consequences of the lack of control:</td>
<td>21</td>
</tr>
<tr>
<td>Providing control: What are the perspectives?:</td>
<td>23</td>
</tr>
<tr>
<td>Right to Informational Self-determination:</td>
<td>23</td>
</tr>
<tr>
<td>Behavioral Economics Perspective:</td>
<td>25</td>
</tr>
<tr>
<td>Preliminary Clarifications:</td>
<td>28</td>
</tr>
<tr>
<td>Which behavior wants to be achieved?:</td>
<td>28</td>
</tr>
<tr>
<td>Experimental issues:</td>
<td>29</td>
</tr>
<tr>
<td>Important concepts:</td>
<td>30</td>
</tr>
<tr>
<td>Bounded rationality:</td>
<td>30</td>
</tr>
<tr>
<td>Loss aversion:</td>
<td>33</td>
</tr>
<tr>
<td>Time inconsistency:</td>
<td>34</td>
</tr>
<tr>
<td>Bargaining impasse and self-serving bias:</td>
<td>35</td>
</tr>
<tr>
<td>Confirmatory bias:</td>
<td>35</td>
</tr>
<tr>
<td>Providing data processing information:</td>
<td>39</td>
</tr>
<tr>
<td>Unifying the information:</td>
<td>41</td>
</tr>
<tr>
<td>A value-oriented model of data management:</td>
<td>44</td>
</tr>
<tr>
<td>How valuable is the data?:</td>
<td>44</td>
</tr>
<tr>
<td>What do we get with providing value?:</td>
<td>45</td>
</tr>
<tr>
<td>Value vs. Property:</td>
<td>47</td>
</tr>
<tr>
<td>Conclusion:</td>
<td>48</td>
</tr>
<tr>
<td>II. Bibliography:</td>
<td>51</td>
</tr>
</tbody>
</table>
Rethinking Informed Consent:

Giving back control to the data subject from a behavioral economics perspective.

Introduction:

It is safe to say that the notion of controlling the destination of one’s personal information has been strongly involved in the development of the data privacy/data protection discipline. The right to informational self-determination, developed in Germany during the 1980’s, entails a value that is still transversal in history; that a person should be able to limit the information that can be used of himself. The American tradition has long recognized equivalent values, identifying the right “to be let alone” as a way to promote a non-intrusive information gathering against the media and the emerging technologies, and as a right grounded in the control of the individual to determine what information can be openly communicated.

On paper, the European legislation has included several provisions which goal seem to provide more control of the information for the data subjects. Indeed, the former Data Protection Directive (from now on the “DPD”) and the recently issued General Data Protection Regulation (From now on the “GDPR”), contain the basis to prevent practices that may constitute an illegitimate processing of data, and dedicate several provisions to the possibility of control of the data subject grounded on the informed consent. Nevertheless, the reality of the online scenario has shown the inability of this model to provide control and to protect the data subject’s right to privacy.

---

1 Professor Lee A. Bygrave has a thoughtful definition of the field of data privacy law, and the meeting points and dissimilarities between different terms that compose the field, such as “data protection”, “data privacy” and “data security”. For conceptual purposes, this work will indistinctively use the terms “data protection” and “data privacy” to address, in the words of professor Bygrave, the regulation of “(...) all or most stages in the processing of certain kinds of data” as well as “(...) the ways in which the data is gathered, registered, stored, exploited and disseminated”. See: (Bygrave, 2014, pp. 1-5)
2 (Schwartz, 1989, pp. 678-689)
3 (Warren & Brandeis, 1890)
4 (Warren & Brandeis, 1890)
5 The European Parliament and the Council of the European Union. Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,
6 The European Parliament and the Council of the European Union. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
As will be argued in the following lines, part of this situation has been prompted with private interests in mind and with acquaintance of public actors, by creating conditions that have slowly undermined the capacity of the users “to be let alone” at their will. Indeed, the activity of data processing is an important tool for profit, used by corporations that benefit from advertisement\(^7\), with little to no benefits for the users and, in several cases, with detriments and sacrifices, such as unwanted publicity of private life\(^8\) and clandestine surveillance\(^9\).

Among experts, there is a debate if whether providing more control to the data subject can be a solution applicable in the real world for the protection of the right to privacy. The critics of a control-oriented approach base their arguments on the practical, conceptual and moral difficulties of the model\(^10\), but mainly on the fact that the consent, as the main mechanism of control of the data subject, has so far proved to be impractical and inefficient\(^11\).

A concise reason for this failure is still subject to debate. Some, especially in the private sector, believe that the modern society is currently suffering a transition, where the traditional concept of privacy, or privacy as a “social norm,” is being dismissed with the excuse of an interconnected world\(^12\). Although this explanation is convenient for businesses, it also disregards the fact that society has become increasingly more suspicious of the use that companies are giving to their information\(^13\).

On the other hand, it must be taken into account that a position that relies heavily on theoretical issues by giving a disproportionate and unrealistic value to the right to privacy, may dismiss the reality of the online environment. Any current analysis and critic of the model of data processing must consider that the reality of the internet requires accepting the paramount and omnipresent

---

7 (Packin & Lev-Aretz, 2016, p. 1230)  
8 (Barbas, 2012, p. 981)  
9 (Tsesis, 2014, p. 438)  
10 (Allen, 2000)  
11 (Koops, 2014, p. 3)  
12 On 2010, with the rapid increase in the use of social media, Mark Zuckerberg, founder of Facebook, stated that privacy was no longer a “social norm”, as social media sharing reflected a change in attitude. See: (Johnson, 2010)  
13 Several polls have shown the rejection of the public in relation to surveillance and data gathering. These polls will be discussed in Section 1.2. See: (Jourová, 2015) (Madden & Rainie, 2015)
value of data and information, not only as commercial assets\textsuperscript{14} but also as important factors to implement public policies\textsuperscript{15}.

This scenario presents us with a difficult dichotomy: From one side, the social perception seems to prove a general concern of the public in relation to the use that private actors make of their data while, at the same time, legislators continue tailoring rules that favor business interests and allow an almost unrestricted use of data, with weak possibilities of control for the users.

Moreover, the disconnection of social perception with reality shows that the optimistic approach of cyberspace as a tool for democratization is today, more than ever, a questionable assumption\textsuperscript{16}. Noam Chomsky and Edward S. Herman, in the introduction to the 2002 edition of the influential work “\textit{Manufacturing Consent}”, noticed the big limitations of the Internet as a critical tool, in the sense that “(T)he audience “interaction” facilitated by advancing interactive capabilities mainly help audience members to shop, but they also allow media firms to collect detailed information on their audiences, and thus to fine-tune program features and ads to individual characteristics as well as to sell by a click during programs. Along with reducing privacy, this should intensify commercialization.”\textsuperscript{17}

The possibilities and dangers of the massive collection of data by private companies with overriding economic interests cannot be undermined. Lessig is illustrative in pointing out that, “\textit{left to itself, cyberspace will become a perfect tool of control (…) not necessarily control by government, and not necessarily control to some evil, fascist end (…) the struggle in that world will not be government’s. It will be to assure that essential liberties are preserved in this environment.”\textsuperscript{18}

What this work aims to show is that, although the legal concepts of privacy between the predominant Western traditions contain discrepancies mainly in their formation, they are not so different in their outcome, as Western traditions embrace the concept of control of the data subjects as a capital guideline of data protection.

\textsuperscript{14} (Clifford, 2014, p. 196)
\textsuperscript{15} (Eberle, 2001, p. 970)
\textsuperscript{16} (Megenta, 2009-2010, p. 4)
\textsuperscript{17} (Herman & Chomsky, 2008, p. 31)
\textsuperscript{18} (Lessig, 2006, p. 4)
Moreover, the following work aims to prove that in the current state of affairs, the weak and sometimes inexistent control of people over their information has not been the product of a social and cultural transformation, but that, instead, it is an answer to external pressures of economic and political nature. This analysis aims to conclude that the negative social perception of the data processing for commercial purposes, and the potential dangers that such activity entails for freedom and democratic values, should lead to reconsider the direction of the current legal regime.

This thesis would analyze the right to informational self-determination as a proposal directed to provide control to the data subjects, recognizing that such measure, in practice, may not create and actual empowerment of the users.

As an alternative proposal, or even as a complement for the advocates of the right to informational self-determination, the work will analyze the possibility of implementing a system that provides better control for the data subjects, but that requires a different starting point.

This starting point demands to analyze the implications of the field of behavioral economics and legal economics in the data privacy scenario. The goal of implementing a behavioral economics perspective is to create a conscientious decision-making scenario for the users. The objective of this analysis is to restore the position of the concept of informed consent as the primary way of control for the data subject, while recognizing that to achieve such informed consent, the data subject must be provided with more suitable conditions.

This work will analyze a proposal for the creation of such a suitable scenario, first with implementing alternative ways to provide information to the data subject. Furthermore, the creation of such scenario requires shifting the model of exchange of data, by providing a value from a consumer’s perspective. It will be argued that this model may create awareness and responsibility but, at the same time, recognizes the paramount economic and social importance of data processing in the current state of development of the technology industry.
1 Privacy in Western traditions: A story about finding and losing control:

1.1 Privacy as control:

An exposition of the right to privacy should start recognizing that, as Professor James Q. Whitman states, “the concept of privacy is embarrassingly difficult to define.”19 One of the probable causes for this statement is that the notion of privacy raises different connotations depending on social and legal traditions, mainly the Western traditions of Europe and North America.

Different factors, like the variance in the development of press and media, created disparities in social sensitivity between Europe and North America. Samantha Barbas accurately states that “privacy law did not develop strongly in America because its evolution coincided with the emergence of a liberal free press doctrine and a culture of exposure.”20

Nevertheless, the assumption of the American tradition as a one that does not encourage or embrace privacy is also incomplete. It is more accurate to conclude that the conceptions of privacy between Western traditions simply differs in fundamental matters that, at some point, may be interchangeable in their outcome, although not very often in their foundation.

Indeed, according to Professor Whitman, the concept of privacy in the European tradition is seen as a right, strongly attached to human dignity, that implies the control of information that can be disclosed about an individual21 In this context, the enemy of privacy is broadly understood as any person, natural or legal, that in some way acquires information and aims to disclose it. More importantly, the European concept of privacy deeply embraces the ability to control the information.

On the other hand, the American conception of privacy entails freedom from the intrusion of states and contains a deeper distrust of public agents than private agents22. Moreover, the American recognition of privacy, due to European influence, also adopted the concept of control of information as an important value. The main and most influential basis for the modern conception of privacy in the United Stated originates from Samuel Warren and Louis Brandeis´ article “The

---

19 (Whitman, 2004, p. 1153)
20 (Barbas, 2012, p. 1018)
21 (Whitman, 2004, p. 1161)
22 (Whitman, 2004, p. 1018)
Right to Privacy.” In this article, foreseeing the big impact that newly developed technological devices would have in the lives of individuals, mainly instantaneous photography of the media, Warren and Brandeis embraced the right “to be let alone,” as an extension of the inviolability of personality. But with the recognition of the right “to be let alone”, Warren and Brandeis consequently embraced the need of control of the subject that creates the information:

“The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others (...) the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone.”

Professor Whitman notices the big influence that the European tradition had in Warren and Brandeis, by proclaiming the dangers of losing the capacity of control over personal information. In other words, the concept of human dignity of the European tradition, in one way or another, has also deeply influenced the conception of privacy in America.

The importance of having control of the information and the dangers of mass data processing have been thoroughly recognized both in America and Europe during the XX Century. The influence of state policies arguably helped in the development of a control-oriented perspective. Indeed, one of the main influences for the modern concerns and regulations of data processing originates with the use of statistical techniques of computer data processing by the Nazis, with the purpose of identifying Jewish during the 1930’s. This important precedent anticipated the cooperation of state agencies with top-notch technology companies (IBM in this case) for surveillance and profiling activities.

The dire consequences of the categorization and profiling performed by the Nazis certainly influenced the social perception of data processing in the years to come. It is considered that the

---

23 (Krause & Marcus, 1977-1978, p. 377)  
24 (Warren & Brandeis, 1890)  
25 (Whitman, 2004, p. 1167)  
26 (Akrivopoulou & Psygkas, 2011, p. 262)  
27 (Black, 2002)
strong protection of privacy in Germany, with the creation of measures such as the right to informational self-determination, has been a reaction to the Nazi and Communist eras\textsuperscript{28}.

A parallel control-oriented development occurred in the United States during the XX Century. As an example, in 1969, the famous Nader Report elaborated to examine the functioning of the Federal Trade Commission in the United States, raised several privacy concerns in relation to data mining. This report already foresees that the increase of mass data processing and the joined use of social-psychological analysis of potential markets affected the privacy and autonomy of the consumers\textsuperscript{29}. While recognizing the importance of the user’s autonomy over the information, the report warns of the potential of mass processing of data for marketing practices as a form of social control, due to the possibility of creating normative patterns in the users\textsuperscript{30}.

This section has shown that although the different Western traditions may have dissimilarities in the concepts that ground the right to privacy, there is a similar outcome, in the sense that privacy, as a right or as freedom, has been strongly linked with the idea of control. Professor Anita L. Allen, in spite of criticizing the concept of control in the data privacy field as unnecessary and staggering, recognizes its importance as a consensual paradigm in the academy\textsuperscript{31}.

Professor Paul Schwartz notices that the attempts to create limits and regulate the processing of data should not depend on the legal idea of privacy, but it should rely on the effects that the information processing can have in human autonomy\textsuperscript{32}. This thesis believes that the effect that Schwartz declares should be oriented to the possibility of autonomously controlling the destination of data and information.

1.2 **Privacy as control: Outdated or ignored?**

The increasing technological developments and the generalized processing of data that disregards a classical conception of the right to privacy of the data subjects has led some to identify a change in the social perception of privacy, in support of a laxer view that benefits an interconnected world. In support of a new and broader concept of privacy, Facebook’s CEO and founder, Mark

\textsuperscript{28} (Cole & Fabbrini, 2016, p. 177)  
\textsuperscript{29} (Hasty, 2014-2015, pp. 307, 308)  
\textsuperscript{30} (Silbey, 1984, p. 454)  
\textsuperscript{31} (Allen, 2000, p. 864)  
\textsuperscript{32} (Schwartz, 1989, p. 676)
Zuckerberg, stated in 2010 that “(P)people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.\(^{33}\)”

Now, it is undeniable that the concept and perception of privacy have dramatically evolved during the last decades. An interesting example of this change occurred during the 1980’s in the United States, when phone companies implemented the Caller ID system, by which the recipients were able to know the phone number of the other line after paying an additional fee for the service. The main issue in this debate was whether the phone companies had the right to disclose information of the users or if the users were the ones entitled to said right\(^{34}\). The strong rejection of the public in this matter led to the creation of a service of free per-call blocking that made the phone number unavailable and provided better control for the users on when to disclose personal information\(^{35}\).

Nowadays this system seems meaningless for the protection of privacy, as the identification of incoming calls is a current standard in pretty much any mobile telecom operator. On the 1980’s, nonetheless, the social perception of privacy required more stringent measures of control.

Nevertheless, the fact that in the past there was a broader understanding of the information that was considered important for the users, not necessarily means that people have dismissed the possibility and need of control and the importance of privacy and anonymity.

A survey made by the European Commission on June 2015 on 28.000 EU citizens, showed that a 67% percent of the respondents were concerned about not having control over the information they provide on the internet. The survey showed that although 71% percent of the respondents accept that providing information is part of modern life, the majority of the people still feels uncomfortable about the fact that companies use this information to tailor advertisement. It is interesting to notice that, in comparison to the same survey done in 2010, there is not a substantial change in perception.\(^{36}\)

\(^{33}\) (Matyszczyk, 2010)
\(^{34}\) (Rotenberg, 2001, p. Rec. 12)
\(^{35}\) (Rotenberg, 2001, p. Rec. 14)
\(^{36}\) (European Commission, 2015)
A similar survey done in the United States on early 2015 showed an even higher distrust in the activity of online service providers. This survey showed that for more than 93% of adults it was important to have control over who can get their information, and 90% considered important to have control over the type of information that can be collected. The survey also evidenced that the majority of respondents have little trust that online service providers keep the collected information private and secure and, interestingly enough, 55% believe that people should have the ability to use the internet in a completely anonymous way. Arguably, a higher level of concern shown in the American survey is an answer to the Snowden revelations of the collection of data by the NSA.

In any case, this information shows the contradiction between the perception and concerns of the public, with the real life application of data processing. A big part of the problem lays on the fact that, as accurately stated by Lilian Edwards, “users care deeply about their privacy but can’t be bothered to read privacy policies.”

Moreover, technological companies have encouraged a gradual change in perception, aiming for a broader acceptance of data processing. An interesting example is provided by Google, who, after constantly stating that the different services of the company (Youtube, Gmail, etc.) would never correlate data as a way to enhance privacy, in 2012 announced the combination of the data gathered across all platforms in order to create a better profile of the user.

But regardless of the concerns that online users show for the processing of data, currently it is virtually impossible to browse the web anonymously, and the possibility of control has generally been dismissed. The notion that “law is what works, what seems appealing and appropriate in a given society” or that “the law also aims to express social values”, deeply lacks in the field of data privacy and proves that there are no few cases in which the legal recognition of social values is ignored to favor private and economic interests.

37 (Madden & Rainie, 2015)
38 (Edwards, 2013, p. 25)
39 (Mara, 2004)
40 (Kang, 2012)
41 (Villas-Boas, 2015)
42 (Whitman, 2004, p. 1168)
43 (Whitman, 2004, p. 1170)
2 Current state of affairs: An unbalance between regulation and social perception:

The proposal to modify the DPD introduced on 25 of January 2012, had, as one of its main aims, the idea to strengthen the online privacy of the users. As stated by the EU Justice Commissioner Viviane Reding, “(M)y proposals will help build trust in online services because people will be better informed about their rights and in more control of their information.” It is interesting to notice that the concept of control has been even embraced by the European Union when drafting the original proposal for the GDPR. Nevertheless, this possibility, in practice and in the way it was adopted, seems not to provide enough protection or control.

There are several lawful basis for the processing of data according to Article 6 of the GDPR, including legal obligations and the protection of the data subject’s interests. This work, as it concerns with the concept of control of the data subject, will focus on the current state of affairs of the consent as a ground for data processing. The reason for this is that currently, consent is the main tool to legitimate data processing, and the primary tool for the data subject to exercise any control.

Now, strongly attached to the consent of the data subject, the GDPR introduces the right to be forgotten as a tool of control of the data subjects.

The following section will briefly focus on the consent and the right to be forgotten among other mechanisms, and will analyze the suitability of these mechanisms to achieve an actual control of the data subjects. Also, this section will briefly study how different external pressures have deeply influenced the outcome and current implementation of the mechanisms of data privacy of the GDPR.

2.1 Consent:

In an optimistic approach, Jessica Rich, Director of the FTC’s Bureau of Consumer Protection, stated that provided enough information, the user must be able to decide if the benefits of a service worth the information that the user is providing in exchange. This statement should not be

---

44 (European Commission, 2012)  
45 (Enerstvedt, 2015, p. 1)  
46 (Flaherty, 2013)
considered lightly, as it is true that a properly informed consumer should have the autonomy to decide if subscribing to a service in exchange of his data. Nonetheless, the main problem in shaping this informed consumer has been linked to the inability to create mechanisms that encourage such behavior.

Article 4 (11) of the GDPR, defines that consent “(...) means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

The concept of consent adopted in the GDPR relies on perfectly valid grounds, and contains legitimate aims, in the sense that it should be freely given and informed. Nevertheless, so far, the model of implementation of consent that provides control to the data subject and the tools for this end have been inconvenient and not appropriate for the purpose.

It is worth mentioning an interesting experiment that was performed by the Norwegian Consumer Council, where volunteers read the terms of use and privacy policies of the apps of an average Norwegian smartphone. The process of reading the terms of use and privacy policies of 33 apps containing around 250,000 words, lasted more than 24 hours, and led the Norwegian Consumer Council to the obvious conclusion that “mobile apps' terms of use and privacy policies fail to uphold privacy obligations and users' consumer rights.” Moreover, it shows an evident problem on the concept of consent, due to its impracticability, even for the most dedicated and responsible users.

A big part of the problem lays in the outdated nature of the current model of consent. As stated by the privacy advocate Simon Davies, “most consent mechanisms were conceived in the pre-dawn of the Internet age. They were developed at a gentler time in history – a time when it was possible to build a simple flow chart of personal data relationships.”

---

47 For more information about the experiment, see: (The Norwegian Consumer Council, 2016)
48 (The Norwegian Consumer Council, 2016, p. 4)
49 (Davies, s.f.)
But even if it is accepted that consent, as drafted in the GDPR, is a proper tool for control, other provisions further diminish the autonomy of the data subject. Indeed, Article 6 (4) of the GDPR allows the processing of data for purposes that have not been subject to the consent of the data subject, as long as the controller proves compatibility between the initial and the new purposes. The criteria to determine such compatibility (Article 6 (4) (a-e)) are conspicuously broad, with plenty of space for interpretation.

With reason, critics of a consent-based approach point out its lack of suitability as a practical solution for the problem of the lack of control of the data subject. Some of these critics aim to prove that the concept of consent is currently an illusion, as the users give it in non-negotiable, non-informed and pressurized basis. In a broader way, some authors believe that the sole concept of control is an illusion, since data subjects constantly and willingly disclose their information.

Professor Anita L. Allen, for example, stresses the practical difficulties of providing control on the ground that “control over personal data appears to be neither necessary nor sufficient for states of privacy to obtain,” since people that may have control over their information, choose to give up this faculty.

This work agrees with the fact that the consent, left alone and in the way it has been implemented, is not a proper tool for providing control and often denies the reality of the online context. Nevertheless, denying the role of consent as a valuable ground to provide control for data subjects, as some researchers have concluded, seems an extreme position. A realistic approach to the protection of data from the point of view of a control-oriented model, should not stop relying on the consent and the judgment of the data subjects.

It is clear that in the current online context, consent is not a practical solution. But the reason for this does not fall in the uselessness of the consent in itself, but because the design of the data processing model does not provide enough tools to empower the users. This thesis considers that a viable proposal for providing control to the data subjects should have as a starting point the

---

50 (Koops, 2014, p. 3)
51 (Edwards, 2013, p. 24)
52 (Allen, 2000, p. 869)
53 (Allen, 2000, p. 869)
54 (Allen, 2000, p. 867)
55 (Koops, 2014, p. 4)
consent. But said consent should be designed in a way that provides a real possibility to decide of the data subject.

The position of this thesis, shared by other authors in the field\textsuperscript{56}, is that the consent is a valuable and important tool for the data subject that should not be easily disposed on the grounds of attaining to reality. On the contrary, the concept of consent should maintain its importance in the data protection field, but its direction and implementation should be reconsidered.

2.2 Other mechanisms of control.

In addition to the importance of consent as a tool of control, other mechanisms were implemented in the GDPR that seem to follow this same end.

One of the most important measures is the inclusion of the “right to be forgotten”, understood as the right of the data subject “to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation\textsuperscript{57}”

During the process of drafting, the proposal for a “right to be forgotten” was received by some with strong optimist, even stating that the proposal was the first legislative measure that included a right to property on the personal data\textsuperscript{58}.

Although this new right seems to strengthen the possibilities of the data subject to have control over the data, it is not an allowance for anonymity, and it is subject to broad exceptions, as follows:

\textquote{the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health,}

\textsuperscript{56} (Staben, 2012)
\textsuperscript{57} GDPR. Recital 65.
\textsuperscript{58} (Victor, 2013)
for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defense of legal claims."

Even while assuming that the inclusion of this new right seeks to provide control for the data subject, the mechanisms to achieve this aim are simply not appropriate.

Besides of the broad exceptions for the application of this right, critics can also be ground on the weak obligations of the data controller. Indeed, in case the user decides to exercise this right, the controller, when has made the data public, must take reasonable steps to inform of the order of the data subject to other controllers that are processing the data. The fact that the controller is only compelled to take “reasonable steps” to communicate the erasure order and “taking into account of available technology”, creates the possibility of broad interpretations, and seems to disregard and diminish the importance of the data and the need for the controller, as the one who discloses this data, to supervise the destination and maintain a tight control of the information.

Other mechanisms of the GDPR that share an approach of control of the data subject can be even more problematic. For example, Article 21 contains the “right to object automated decision-making”. As with the “right to be forgotten”, broad exceptions are included that hardly provide any control for the data subject. As drafted in the GDPR, the controller may continue processing the personal data, even after an objection, when there are a “compelling legitimate grounds for the processing”. Different interpretations have found that the expression “legitimate interest” or “legitimate grounds” is a general concept that requires an analysis on a case-by-case basis. It requires an assessment, also called “balancing test” that has to be initially made by the data controller, but more importantly, it has been considered that a legitimate interest of the controller can be interpreted as broadly as to include direct marketing, unsolicited non-commercial messages that include political campaigns, among others.

Finally, it is worth mentioning the “right to data portability” introduced in Article 20 of the GDPR. This provision allows the data subject to receive the personal data that has been provided to a

---

59 GDPR. Recital 65.
60 GDPR. Article 17 (2)
61 (The Article 29 Data Protection Working Party, 2014, pp. 11, 13)
controller. Although it has been stated that this right enlarges the informational self-determination and provides control for the data subject\textsuperscript{65}, there are also problems with its application.

The main issue with the implementation of this mechanism, issue applicable to the other mechanisms of control mentioned in this section, is the fact that with the current legislative measures, this right is difficult to be exercised since the beginning, as users are not aware of the steps of the data processing. As accurately stated by Eva Fialová, “\textit{(T)he control may be exercised by the individual if only he/she is aware of the rights and of the means to claim those rights. Without awareness of the right, this right becomes meaningless in practice. The control cannot be maintained in case of the individual's ignorance in relation to a particular legal instrument.}”\textsuperscript{66}

Indeed, the sole process of data gathering and the further steps of processing\textsuperscript{67} are, in most cases, performed on the basis of a weak and uninformed consent, where data subjects are unaware of said processing. Indeed, “\textit{most users are not even aware that the web sites they visit collect user information, and even if they are cognizant of that possibility, they have little conception of how personal data might be processed}”\textsuperscript{68}. In this way, a mechanism that allows the data subjects to obtain their information faces several challenges, since the data subjects are unaware of the identity of the controllers or even of the sole fact that the data is being gathered.

Moreover, the consequences of data processing are not immediately evident or are hidden to the public, leaving the knowledge of the data subjects adrift, lacking legal remedies to protect their privacy.

These provisions show that the wording of the GDPR, that on paper seems even to approximate the data as and object subject to property, contains exceptions that greatly limit their extent and original purpose. Stating, as some do, that “\textit{although data is a kind of commodity capable of changing hands, the data subject always retains the ultimate entitlement to this property,}”\textsuperscript{69} it is simply not accurate in the current online scenario.

\textsuperscript{65} (Fialová, 2014, p. 46)
\textsuperscript{66} (Fialová, 2014, p. 47)
\textsuperscript{67} GDPR, Article 4 (2), defines processing as any activity on personal data that goes from the “\textit{collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction}”
\textsuperscript{68} (Netanel, 2000, p. 476)
\textsuperscript{69} (Victor, 2013, p. 525)
2.3 Data protection regime: The unbalance between regulation and social perception:

The previous sections have made evident different problematic issues. One of this issues is the fact that the concept of control of the data is still an important ground for the right to privacy in Western traditions, both from the academic and the social point of view. On the other hand, Sections 2.1 and 2.2 showed that the different mechanisms of control included in the GDPR in the way of consent, “right to be forgotten”, “right to object processing” and “right to data portability”, have not contributed to create a better suited and rightly entitled data subject

The disparity shown on the previous sections between the ideal of control and the real practice of data mining and processing is largely a result of outside pressure and economic interests.

It is interesting to notice how the efforts of the OECD in the elaboration of the “Guidelines on the Protection of Privacy and Transborder Data Flow,” were primarily driven by economic interests. Indeed, the effort of creating the Guidelines mainly answered to the need of establishing a set of principles that would guard against economic protectionism\textsuperscript{70}. The influence of the OECD's instrument has been extensive and can be found in the Safe Harbor Agreement of 2000 between the European Commission and the US Department of Commerce, invalidated by the Court of Justice of the European Union\textsuperscript{71}, and in the data privacy laws of several countries outside Europe\textsuperscript{72}.

This is also true in the context of the European Union with the creation of the former DPD. Indeed, as stated by Professor Lee A. Bygrave, the European Commission, although partly motivated by the protection of human rights, was mainly aiming to eliminate barriers to the realization of the internal market\textsuperscript{73}. The purpose of the DPD is ambivalent, as expressed in Article 1, which, at the same time that protects fundamental rights and freedoms of natural persons, prohibits any restriction in the free flow of personal data\textsuperscript{74}. The aims of the new GDPR for this matter are very similar to those of the DPD.

The value of information as a fundamental economic asset is a fact that companies have assimilated for several decades. Therefore, it is not a surprise the influence of the private actors in the adoption

\textsuperscript{70} \textit{(Bygrave, 2014, p. 43)}
\textsuperscript{71} \textit{(Case C-362/14 Maximillian Schrems v Data Protection Commissioner, 2015)}
\textsuperscript{72} \textit{(Bygrave, 2014, p. 50)}
\textsuperscript{73} \textit{(Bygrave, 2014, p. 55)}
\textsuperscript{74} \textit{(Bygrave, 2014, p. 57)}
of the proposal of the GDPR, which took more than three years due to the intense lobby. Indeed, the GDPR was one of the most lobbied legislations in Europe\textsuperscript{75}, with 3999 amendments only by the Civil Liberties, Justice and Home Affairs Committee\textsuperscript{76}.

The current American approach to the processing of data has also been subject to different pressures that diminish the control of the data subjects. The American legislation, in scenarios not only limited to data protection, has been greatly influenced by economic elites and organized groups representing economic interests, while the average citizen has little to no influence in the elaboration of public policies. This phenomenon has been called an Economic-Elite Domination\textsuperscript{77}.

Nevertheless, external pressure may not only come from private actors, but the public sector has also created important scenarios for questionable data processing. Arguably, one of the most important cornerstones of the current model of data processing and the deterioration of the possibility of controlling data originates in the 9/11 terrorist attacks. From one side, companies that lost their data in the attack in a pre-cloud era realized the importance of their costumer’s information as an economic asset\textsuperscript{78}. But on the other hand and more importantly, the attack created the basis for the infamous Patriot Act\textsuperscript{79}, which changed the rules of the game, not only in the field of law enforcement and counter-terrorism in the digital era but also in the private field of the commercialization of data.

Due to the 9/11, the NSA, with the help of legislative measures, created extensive networks of collaboration with telecommunication companies\textsuperscript{80}. The Protect America Act of 2007, reinvigorated by the FISA Amendments Act of 2008\textsuperscript{81}, gave immunization to private companies that voluntarily cooperated with the US intelligence, culminating in the PRISM program, which managed to create partnerships with Microsoft, Google, Yahoo, Facebook, among several others\textsuperscript{82}. This immunization gave the service providers the possibility to gather information as never

\textsuperscript{75} (European Digital Rights (EDRi), 2016)
\textsuperscript{76} (Albrecht, 2015, p. 1)
\textsuperscript{77} (Gilens & Page, 2014, p. 565)
\textsuperscript{78} (Tucci, 2013)
\textsuperscript{79} (Department of Justice (USA), s.f.)
\textsuperscript{80} (Laberge, 2010, p. 97)
\textsuperscript{81} (Laberge, 2010, p. 96)
\textsuperscript{82} (Gellman & Poitras, 2013)
before\textsuperscript{83}, creating an auspicious ambient for arbitrary data processing of private companies. In words of Peter Hustinx, in the post 9-11 model “many business practices online, including some of the most popular ones, are also based on extensive monitoring of consumer behaviour, and that the growing practice of providing 'free' services in exchange for monitoring has created opportunities for large scale spying by other actors\textsuperscript{84}.

The main concern with the external pressures that have so far, molded the modern data processing regime is their unawareness of the data subjects’ rights. Nonetheless, it is important to recognize that fundamental rights, as the right to privacy, cannot be considered absolute\textsuperscript{85}, and that a proper balance between said rights and economic interests or values of another kind is often required. It is for this reason that the Article 52 of the Charter of Fundamental Rights of the European Union allows the limitation of the rights and freedoms contained in the instrument, as long as the limitation is provided by law and it is subject to the principle of proportionality. The application of the principle of proportionality implies that the measure must be necessary and adequate for its objectives\textsuperscript{86}.

Nevertheless, the capital importance of protecting fundamental rights in the field of data privacy must not be easily disregarded. The Court of Justice of the European Union has expressed the following:

\textit{“It should also be noted that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights.”}\textsuperscript{87}

As stated by the Court, the activity of data processing should, at its core, contain considerations of the fundamental rights. A realistic and proportional approach implies to consider that the data

\textsuperscript{83} For more information in relation to the data processing practices of private companies in the post 9/11 legal regime, see the documentary: (Terms and Conditions May Apply, 2013).
\textsuperscript{84} (Hustinx, 2014, p. 2)
\textsuperscript{85} (Vries, 2013, p. 170)
\textsuperscript{86} (Vries, 2013, p. 177)
\textsuperscript{87} (Joined cases C-465/00, C-138/01 and C-139/01. Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk, 2003), Recital 68.
processing, in a general way, has become an important economic activity, but that such activity must also be respectful of the fundamental rights of the individuals.

2.4 Consequences of the lack of control:

Very often, and with the acquaintance of technology companies, the information that users have of the negative consequences of data exchange and monitoring is diminished. As seen above, Facebook’s Mark Zuckerberg believes that sharing, and not privacy, is the new social norm.\(^88\) This statement, not only disregards the actual perception of people but also dismisses the issues that may arise with the lack of control.

In reality, the production of generalizations on profiles increasingly leads to unfairness in social interactions, where individuals are treated as indivisible parts of reference groups. For example, in non-distributed generalizations and profiles, data subjects may be refused loans based on the reference group where they have been classified, even if the individual does not exhibit every property of said group.\(^89\) Such cases raise concerns about the potential of profiling in the determination of social classes and the encouragement to discrimination and control of individuals.

The use of profiling tools also has the potential to threaten democratic values by affecting people’s decision making. Indeed, the creation profiles is increasingly being used to disseminate specifically tailored information to the users that can certainly influence their behavior and limit their choices.\(^90\)

The same capability of molding behavior can, and it is being used for the prevention of what is considered anti-social behavior. The creation of children profiles allows the identification of “odd behavior” and aims to inhibit and adapt the child to certain social standards.\(^91\) In these cases, the determination of social standards raises important concerns for the freedom and development of individuals and presents even bigger challenges to democracy.

Moreover, the activities of mass surveillance of public actors are increasingly possible due to the information gathered by private entities. An example of this is the revelation of the large scale monitoring of online behavior by the US National Security Agency and other intelligence services,

\(^{88}\) (Matyszczuk, 2010)
\(^{89}\) (Vedder, 1999, p. 277)
\(^{90}\) (Eberle, 2001, pp. 970-972)
\(^{91}\) (Simitis, 1987, p. 713)
as well as by private corporations\textsuperscript{92} and the collaboration of both private and public actors for this purpose. In the context of the war on terror, preventive measures based on racial, ethnic and national profiles\textsuperscript{93} arguably encourage social exclusion and create discretionary and sometimes arbitrary powers in the public authorities.

Other psychological effects of the perception of being monitored have been identified. Indeed, the latent, even if not certain possibility of being monitored defines people’s decision-making and behavior, often by abstaining of acting in a certain way with the idea of being observed, gravely affecting people’s freedom to access information and content\textsuperscript{94}.

As Hayek accurately stated in “The Road to Serfdom,” depriving individuals of their individuality is the best tool to concentrate and height power and to create totalitarian powers\textsuperscript{95}. What Hayek argues is that concepts like private property and other means of control of the individuals are, at the same time, the best guarantee of their freedom\textsuperscript{96}. In the current model of commercialization of data, this concept has not lost any validity but has gained even more importance in a moment where individuals have lost control over their information, and where such information is used in countless ways to create real legal consequences.

Certainly, there are innumerable positive applications that can arise from profiling and the collection of data. Professor Simits mentions an early example, with the program “Gériatrix” in France, that aimed to determine the degree of autonomy of an elderly person in a hospital, indicating the state of the patient and, therefore, creating individualized information that helps to reduce personnel costs and creates better and more personalized services for the patients\textsuperscript{97}.

The positive applications of the processing of personal data and the creation of profiles can and must be exploited. Nevertheless, it is important not to ignore the dangers that entail the collection of data, especially in a society increasingly more distrusting of the online environment, but without the tools to actively protest and correct this situation.

\textsuperscript{92} (Hustinx, 2014, p. 2)
\textsuperscript{93} (Pap, 2010, p. 288)
\textsuperscript{94} (Eberle, 2001, p. 970)
\textsuperscript{95} (Hayek, 2005, p. 42)
\textsuperscript{96} (Hayek, 2005, pp. 40, 41)
\textsuperscript{97} (Simitis, 1987, p. 709)
3 Providing control: What are the perspectives?

As it has been analyzed in the previous sections, the idea of control of the data subject is not new, but it has been attached to the right to privacy since the moment that Western doctrines identified the threatens that a world increasingly more technological represented.

An important cornerstone in this matter is the German approach, with the right to information self-determination.

3.1 Right to Informational Self-determination:

The right to informational self-determination arguably has its origin in the 1983 Census Decision of the German Constitutional Court. Grounded on the right of personality\(^{98}\), the Court created a constitutional and positive mandate for the state to safeguard human autonomy against the intrusive use of information\(^{99}\). This concept has become so important that for some authors, the notion of informational self-determination, although not a synonymous, it is considered closely linked to the general concept of data protection\(^{100}\). Nevertheless, it is also true that this concept has been usually far from real and practical applications, although it dominates policy and scholarship rhetoric\(^{101}\).

In several aspects of the development of data protection, the right to informational self-determination has been an informative and laudable aim. Regarding defining and directing privacy as a right that entails control of the data subjects, the discourse of informational self-determination has been the most significant\(^{102}\). This is due to the fact that this notion embraces the possibility of people to exercise control over their personal data and the uses or destination of it\(^{103}\). In other words, it states that individuals must have the possibility to control their information if disclosed\(^{104}\).

\(^{98}\) (Staben, 2012)
\(^{99}\) (Schwartz, 1989, pp. 678-689)
\(^{100}\) (Koops, 2014, p. 3)
\(^{101}\) (Koops, 2014, p. 3)
\(^{102}\) (Bygrave, 2014, p. 28)
\(^{103}\) (Koops, 2014, p. 3)
\(^{104}\) (Whitman, 2004, p. 1161)
The implementation of a right to informational self-determination has been proposed in different ways. Some approaches support its recognition as a constitutional right\(^{105}\), grounded on the idea that the Constitution may create a framework for debate within societies, or as a way to enumerate and give fundamental value to the principles that must govern privacy in relation to the gathering of information\(^{106}\). Moreover, this position considers that the right to informational self-determination can be deduced and concretize from the concept of human autonomy and personal freedom\(^{107}\).

The supporters of the inclusion of a right to informational self-determination in the legal system tend to argue that the fallibility of the current data processing regime lays on the inconsistent and episodic response of the legislator\(^{108}\).

The idea of control that these approaches pursue is ideally fair and accurate but has strong drawbacks in practice. The concept of informational self-determination is strongly linked to the concept of consent. “In this approach, any processing of personal data is in principle regarded as an interference with the right to informational self-determination, unless the data subject has consented.”\(^{109}\) As discussed before, the tool of consent as a way for the data subject to authorize the processing of data, has greatly proved its inefficiency in the current model of data processing. Certainly, the inclusion of the right to informational self-determination in a constitutional level, right that is materialized with the consent of the data subject,\(^{110}\) does not seem to be a measure that would create a real-life effect different than complying with a rhetoric and formalistic purpose.

The idea that the sole recognition of the right to informational self-determination in a constitutional level would provide control to the data subjects seems unrealistic in the current online scenario. Territoriality issues that are natural to the online environment prevent the creation of a broad recognition in different territories. It should not be forgotten that “an increasingly globalized world, where the market for goods and services spans national borders, national safeguards and regimes for the protection of personal data or information about individuals is of little value, as

\(^{105}\) (Schwartz, 1989, p. 684)  
\(^{106}\) (Eberle, 2001, pp. 970-978)  
\(^{107}\) (Eberle, 2001, pp. 970-1003)  
\(^{108}\) (Eberle, 2001, p. 1014)  
\(^{109}\) (Hustinx, 2014, p. 8)  
\(^{110}\) (Staben, 2012)
technology allows the information to be whisked out of the jurisdiction at the proverbial click of a mouse.\textsuperscript{111}

Furthermore, an express recognition of the right to informational self-determination does not seem to include new and substantial elements different than the ones included in already recognized rights. Indeed, the right to privacy and data protection have been already included in the legal instruments of the European Union, some of which are considered constitutional.

Since 1950, the “\textit{European Convention for the Protection of Human Rights and Fundamental Freedoms}” has deeply influenced the development of the data privacy regime, by incorporating the right to respect for private life\textsuperscript{112}. Some writers support the idea that this Convention has acquired constitutional level through incorporation, because it has been extensively incorporated in European states in a supra-legal level and sometimes, in an explicit constitutional order\textsuperscript{113}. Additionally, since 1981, the Council of Europe, with the “\textit{Convention for the Protection of Individuals concerning Automatic Processing of Personal}”, constituted the first and only international body with a multilateral treaty that deals with data processing\textsuperscript{114}.

In this sense, this work believes that the inclusion of the right to informational self-determination in the legal system would not have a practical effect in the reality of the control of the people. Critics of the theory of informational self-determination notice its influence in the shaping of data protection policies, but further warn of its inability to recognize the reality of the online scenario in the XXI Century\textsuperscript{115}.

4 Behavioral Economics Perspective:

The previous analysis shows the contradiction between the ideal of control that the public and most legislations embrace, and the actual way in which the activity of data processing has been performed so far. This disparity evidences the influence of Economic-Elite Domination postures

\textsuperscript{111} (Gunasekara, 2006, p. 364)  
\textsuperscript{112} (European Convention of Human Rights, 1950) Article 8  
\textsuperscript{113} (Sweet, 2009, pp. 8, 9)  
\textsuperscript{114} (Bygrave, 2014, pp. 31, 32)  
\textsuperscript{115} (Koops, 2014, p. 3)
in the elaboration of legislations\textsuperscript{116}, as well as other external pressures. The lack of protection of the data subjects’ rights in this model of data processing demands modifications of different orders.

Nonetheless, the challenges in overcoming the current model of data processing cannot be undermined. As professor Koops, from Tilburg University, accurately states, the move from free services to paid services in exchange for a privacy-friendly model is not something that most users want\textsuperscript{117}.

An important conclusion that has been already stated in Section 2.1 is that the model of informed consent, in the way in which it was included in the DPD and GDPR, has failed to provide protection and control for the data subject. Nevertheless, this work considers that the failure of such model does not derive from the inability of the consent to empower the users. Arguably, the main problem in the model comes from the way in which such consent has been implemented, and the fact that the current model of data processing does not allow the users to be fully informed, since the amount of information provided, as it was showed in Section 2.1, is not practical, even for the most responsible data subjects.

This work supports the revitalization of the concept of informed consent as an appropriate tool of control of the data subjects. Nevertheless, the analysis of the informed consent of the previous sections shows that models that may work in theory, very often prove to be unsuccessful in practice. The previous statement does nothing different than recognizing the complexity of the human mind and the effect of such complexity in individual behavior and social environments. Humans do not work like machines and rarely follow ideal models.

The inclusion of a citation from Frederik Hayek in Section 2.4 is not gratuitous. Hayek is arguably a pioneer in recognizing that economics should not be treated as physics or individuals as machines, but concepts like bounded or limited rationality\textsuperscript{118} (explained later in this work), may prove unexpected and counterintuitive outcomes in people’s actions. In other words, Hayek understood that a strict assumption of the rationality of the individual at the moment of choosing between different options is a simplification that is regularly contradicted in practice.

\textsuperscript{116} (Gilens & Page, 2014)
\textsuperscript{117} (Koops, 2014, p. 4)
\textsuperscript{118} (Frantz, 2013, pp. 2, 3)
The field of behavioral economics, since Hayek, relies on the idea of economy and society as complex phenomena. In this sense, behavioral economics seeks to understand the behavior of individuals and its consequences, grounded on the experimental knowledge of the good or bad choices of the people. In other words, it means to reorient the interest of economy, from formal theoretical assumptions to psychology and real human actions.

A behavioral-oriented approach explores the actual human behavior in connection to law over purely hypothetical or ideal scenarios. In comparison with a regular legal analysis, the inclusion of the economic factor, as stated by Posner, “(...) tries to explain and predict behavior of participants in and persons regulated by the Law.” For conceptual purpose, it is worth noticing that the behavioral economic analysis of law, in comparison to the purely economic analysis of law, with Richard Posner as one of the main exposers, arguably seeks to build more realistic assumptions on human behavior. While the standard model of economics is based on strong assumptions such as ideal decision-making scenarios, behavioral economics tests these models in real life situations, to find evidence of the actual behavior of people.

From a legal point of view, behavioral economics seeks to help the functions of law in three different perspectives: from a positive perspective, the economic analysis explains the effects and content of the law; from a prescriptive perspective, the analysis must consider that role of law in achieving a specific goal, such as discouraging a socially undesirable behavior; finally, from a normative perspective, the economic analysis aims to provide basis for the legitimacy and finality of a legal system as a tool for “social welfare”. It implies, thus, a practical approach that should result in encouraging or discouraging certain types of behavior, with social welfare as its finality. In other words, the application of behavioral economics aims, not only to understand but also to shape behavior in a way that allows taking better choices.

119 (Frantz, 2013, p. 3)
120 (Camerer & Loewestein, 2004, p. 39)
121 (Jolls, et al., 1998, p. 1476)
122 (Posner, s.f., p. 2)
123 (Jolls, et al., 1998, p. 1487)
124 (Cartwright, 2011, p. 4)
125 (Jolls, et al., 1998, pp. 1474, 1475)
126 (Cartwright, 2011, p. 3)
In the current state of affairs, the problematic issues presented in the data protection field are arguably creating a favorable scenario for the application of a behavioral-oriented analysis. Indeed, the previous sections have shown that the protection of the data subjects’ rights based on a behavioral perspective has so far being dismissed, due to economic interests and extensive lobby. In this scenario, this thesis believes that a framework that rules the data processing activity from the point of view of the protection of the data subjects must take into account psychological and sociological factors from a behavioral-oriented perspective.

4.1 Preliminary Clarifications:

4.1.1 Which behavior wants to be achieved?:

One of the main contributions of the field of behavioral economics to law is the recognition that "(...) law can be used to encourage socially desirable conduct and discourage socially undesirable misconduct." Indeed, the application of behavioral aspects and psychological experimentation must, at its end, help in the achievement of a better social order from the economic and legal perspectives, both disciplines that are strongly attached.

This task requires that before proceeding with the analysis of certain important concepts in the applications of behavioral economics in data processing, it must be delimited the type of behavior that wants to be shaped.

Theoretically, the model of consent applicable since the DPD and the GDPR should be able to provide enough control for the users under the adequate conditions. What can be inferred from the Sections 2.1 and 2.2, is that the way in which the information is being provided and the few and ineffective tools provided to the users are futile to create a real control. Nevertheless, the concept of consent, as drafted on the different European rules and under the right conditions, may be a tool for users’ empowerment and control.

The GDPR states that consent must be “freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her.” There are no reasons for changing the aims of the GDPR in this matter. Indeed, the desired

---

127 (Korobkin, 2013, p. 1349)  
128 GDPR, Recital 32
behavior for data subjects lays on their possibility to give consent to the data processing, and the fact that such consent is freely given and fully informed. What the followings lines want to prove with the analysis of certain behavioral phenomena, is that there are no incentives for the creation of an actual informed consent, as the legislation has not recognized behavioral factors. In other words, what this work states is that the desired behavior of the data subjects is clear and evident, and it is written in the legislation, but the tools to achieve such behavior are not available or are insufficient.

4.1.2 Experimental issues:

One of the most important changes of the behavioral economics approach in contrast to traditional approaches is that it aims to increase the explanatory power of economy by relying on psychological foundations\(^\text{129}\). This means that, while it is possible to rely on certain assumptions, the ultimate test of the theory must prove accurate or congruent with reality\(^\text{130}\). The main reason for this is that the sole idea of implementing a behavioral approach, especially in the legal field, comes from the challenges and contradictions that the psychological experiments have shown in relation to economic assumptions that have been paradigmatically\(^\text{131}\).

Professor Edward Cartwright states that “(G)ood behavioral economics can involve theoretical research with no experiments. It can also involve experimental research with little or no theory”\(^\text{132}\). Indeed, behavioral economics can be tackled from different scenarios, theoretical or experimental. Nevertheless, a final approach would ideally consider both models.

Now, several concepts enclose the application of a behavioral economics perspective of law. The following section will discuss some of the concepts that may be valuable for a proposal in the data protection field.

The objective of this thesis and the next sections is not to provide experimental information of the behavior of the people with the implementation of a different data processing regime, but only to create a proposal from a different and, so far, unexplored perspective, such as behavioral

\(^{129}\) (Camerer & Loewestein, 2004, p. 3)  
\(^{130}\) (Camerer & Loewestein, 2004, p. 4)  
\(^{131}\) (Aaken, 2014, p. 422)  
\(^{132}\) (Cartwright, 2011, p. 11)
economics in relation to data protection. Thus, the relation of this two disciplines and the accuracy of this proposal would require an actual empirical analysis of the users’ actions on the internet under more inclusive measures, such as the ones proposed in Section 5.

4.2 Important concepts:

The application of behavioral economics has been mainly determined by experimentations of human behavior. From these experiments, certain assumptions have arisen. The following concepts, common in the discipline of behavioral economics, may have valuable applications in the field of data privacy.

It is important to clarify that most of the next concepts have a bias nature. Biases are errors in a person’s perception of reality. As expressed by Daniel Kahneman “(S)ystematic errors are known as biases, and they recur predictably in particular circumstances.”

The fact that biases are errors should not discourage their use as ways of shaping behavior. Indeed, the behavioral approach of law should provide the basis for a legal system oriented to be a tool for “social welfare”. In the context of biases, recognizing the errors that people tend to do in the course of a transaction should lead to identifying better mechanisms for shaping behavior in a way that allows better suited and more responsible decisions of the data subjects.

4.2.1 Bounded rationality:

The concept of bounded rationality recognizes that people have constraints in their rational capacities, which implies that very often, people use “rules of thumb” to make decisions that rely more on automatic impulses than in conscious thinking.

A good explanation of this phenomenon is provided by the Nobel-prize winner, Daniel Kahneman. He distinguishes between two systems of mind: In the System 1, the mind operates automatically with no sense of voluntary control, while in system 2, there is an effortful and demanding mental activity. What is interesting is that the effortless impressions of System 1 tend to be the source for

---

133 (Kahneman, 2011, p. 7)
134 (Jolls, et al., 1998, pp. 1474,1475)
135 (Cartwright, 2011, p. 10)
the conscious choices of System 2. Moreover, the choices of System 1, although may be innate, may also arise with a prolonged practice that creates an automatic conduct.\footnote{136 (Kahneman, 2011, pp. 22, 23)}

In other words, “\(\text{W}\)hen all goes smoothly, which is most of the time, System 2 adopts the suggestions of System 1 with little or no modification. You generally believe your impressions and act on your desires, and that is fine—usually (...) When System 1 runs into difficulty, it calls on System 2 to support more detailed and specific processing that may solve the problem of the moment. System 2 is mobilized when a question arises for which System 1 does not offer an answer”\footnote{137 (Kahneman, 2011, p. 26)}.

This categorization of decision-making systems has an important influence in the way in which consent is provided online. A vital issue with consent is that, in Kahneman’s words, “\textit{we can be blind to the obvious, and we are also blind to our blindness}.”\footnote{138 (Kahneman, 2011, p. 26)} Arguably, ticking boxes of acceptance for the provision of online services on the current state of affairs seems more similar to a choice of the System 1 than one of the System 2. What this means regarding data privacy is that, even while accepting a big number of terms of use, privacy policies and conditions for the use of cookies, the user never consciously reads such terms and conditions or understands their implications. Nevertheless, it should be recognized that this situation of automatic response of online users should not be exclusively blamed on the data subjects, due to the fact that the current model of data processing provides the proper condition for this problem.

The generalized use of cookies provides a good example of a system that, due to its omnipresence, leads to automatic decisions (System 1) of the data subject. Indeed, according to the Article 5(3) of the Directive 2002/58/EC, the user must give his consent to the use of cookies. Although for some authors, the possibility of consenting the use of cookies means a positive change that represents an almost informed opt-in mechanism\footnote{139 (Bond, 2012, p. 215)}, the problem arises with the fact that 50.1\% of all websites on the internet are currently using some type of cookies, while a big part of these sites are the ones that contribute most of the traffic of the Internet, such as Youtube, Amazon, Wikipedia, among others\footnote{140 (W3Techs, 2016)}. The fact that the majority of websites and the most important and
frequently visited on the internet require the users to constantly provide their consent, makes impractical and costly to take a responsible and informed decision, therefore making the acceptance an automatic action of the System 1.

It is also worth mentioning that while the acceptance of the use of cookies requires a costly and imperfect consent described above, the legislation allows the data controller to do without consent when the cookies are considered strictly necessary. The fact that the controller may use cookies even without the users’ consent, which creates in the users a perception of futility in the action of accepting the privacy or cookies policies, further affects the amount of effort that the data subjects will invest in accepting such policies.

It is important to recognize that in several cases, automatic actions may have positive outcomes, especially for repetitive tasks. Nevertheless, in relation to data protection issues, it seems that the impulse of System 1 creates a lack of protection for the users, who have gotten used to respond automatically to activities of data processing that may seriously affect their right to privacy.

The application of a behavioral-oriented perspective in this matter may provide valuable contributions for a different approach. According to the bounded reality concept, “One of the tasks of System 2 is to overcome the impulses of System 1. In other words, System 2 is in charge of self-control.” What this means is that, in a situation where there is an automatic impulse of System 1, such as providing consent for the use of cookies, System 2 can have the power to overcome said impulse, and by overcoming an automatic decision of providing consent, the user may take a better-suited decision.

Therefore, a mechanism that seeks to ensure the right to privacy of the users should, in its foundation, create tools that encourage a conscious and mindful decision-making. The purpose of a measure in this sense is not to create unnecessary burdens for the users or to make online browsing tedious, but to properly inform the users of the nature of the data that it is being processed and the important implications that the activity of data processing may have for them (for this

---

141 See: Article 5(3), Directive 2002/58/EC
See also: (Information Commissioner’s Office, 2012, p. 12)
142 (Kahneman, 2011, p. 28)
implications, see Section 2.4). As will be explained below, the measures to overcome a bounded reality phenomenon may consist in a better provision of information, as well as in the implementation of a value-oriented model that may encourage the users to be more involved in the data processing activity.

4.2.2 *Loss aversion:*

Another interesting phenomenon that may be brought up is the “loss aversion”. This concept understands that people, when facing losses in a certain transaction, tend to give more weight or importance to said loss than to the gains that the transactions may bring\(^{143}\). This concept is better understood when analyzed together with the “status quo bias,” which states that, unless there is a good reason to change, people tend to stick to what they already have, even if the alternative seems more promising\(^{144}\). People, therefore, have the tendency to stay on the safe side, by giving a higher value to what may be lost than to the reward or retribution of the transaction.

In a general way, it is safe to say that one of the main threats to the right to privacy in the activity of data processing is the ignorance of the losses that the unlimited processing of data entails for the data subject.

A control-based model must, therefore, tackle this issue in different ways. As with the phenomenon of bounded reality, the data subject should be informed of the consequences of providing consent for the activity of data processing. The loss aversion phenomenon relies on the fact that people give higher value to their belongings in a transaction. In order to use this tool to shape behavior, the users must be aware both of the losses and the gains of a data transactions.

But, by itself, the sole recognition of the losses and gains may not be enough when there is not a real consequence in the person’s interests, economic or the like. As explained in relation to the bounded reality, the users must be able to take a mindful decision on the provision of data, not inclined to automatic impulses. This situation leads to propose a mechanism that relies on the

\(^{143}\) For more information about the phenomena of “loss aversion”, see: (Tversky & Kahneman, 1991, p. 1038)

\(^{144}\) (Thaler, 2015, pp. 131, 154)
attention of the data subjects by directly affecting their interests. This can be more easily tackled in a value-oriented model.

4.2.3  **Time inconsistency:**

The phenomenon of time inconsistency shows that people tend to grab immediate rewards at the same time that avoid immediate costs. For example, procrastination comes from the avoidance of immediate costs in performing a task, even when performing this task may have future rewards. Overeating comes from embracing immediate rewards over foreseeable problems, such as overweight. In summary, this phenomenon shows that people tend to prefer present or immediate rewards over future costs, and prefer to avoid present or immediate costs, even if they carry future rewards.\(^{145}\)

Regardless of the time inconsistency tendency, people may or may not fall in the model, depending if their acting is naïve or sophisticated. This means that when a person is not aware of the bias, acts in a naïve way, while when there is awareness of the bias, the action of the person may be more sophisticated.\(^{146}\)

The activity of acquiring a service on the internet through consent to provide personal data constitutes an immediate reward. The service, provided immediately, certainly outweighs the negative consequences for the users of providing such data, consequences that in most cases are not clear or evident. Moreover, even if the user has the will to provide a responsible decision, the action of reading terms and conditions would be too costly in comparison to the reward.

In order to expect a responsible behavior from the users in the disposition of data, the information of the data processing must be provided in a less costly way that allows the user to easily identify the different aspects of the activity. More importantly, a less costly solution for the user must also consider a more unified way of data management.

As will be stated later, different issues, such as the way in which the information is currently provided to the data subjects, as well as the fragmentation in such provision of information, and the fact that terms and conditions among service providers may greatly vary, help to create a costly

---

\(^{145}\) (O’Donoghue & Rabin, 2004, p. 224)

\(^{146}\) (Cartwright, 2011, p. 147)
scenario for the data subjects and encourage ignorance and confusion. The different issues that arise from the provision of information and its fragmentation are of paramount importance, and should be tackled if a control-oriented perspective of data processing is to be expected.

4.2.4 Bargaining impasse and self-serving bias:

Another concept that may find an interesting application is the bargaining impasse and self-serving bias. According to this behavior, there is a tendency of people to identify or to consider something as fair when the outcome represents a benefit for them\textsuperscript{147}. Moreover, this tendency shows that people tend to believe that their notion of what it is fair is impartial, so when the other party bargains, this action is considered aggressive and unfair\textsuperscript{148}.

In general terms, users are unaware of the outcome of a transaction that implies the processing of data. In this sense, the tendency to identify fairness or unfairness in a self-serving bias requires knowledge of the value, as well as of the type, degree of sensibility and final use of the data, all these, information that is not easily accessible. In other words, for the users to determine the fairness of a bargain, they should be aware of both the reward (the provision of a service) and the costs and implications of this reward.

This bias or impasse relies on the stringent viewpoint of people when facing a bargain. It also implies that under a better-suited model, this jealous conduct that people have over their belongings may be used to create a more responsible and conscious user. In any case, the possibility of control that this phenomenon brings, not only demands a better provision of information but also requires a real possibility of bargaining of the data subject, which further supports a value-oriented model and a unified system of data management.

4.2.5 Confirmatory bias:

The confirmatory bias implies that individuals tend to rate positively new information that is consistent with their initial opinion, and negatively the information that contradicts said initial

\textsuperscript{147} (Babcock & Loewenstein, 2004, p. 326)
\textsuperscript{148} (O’Donoghue & Rabin, 2004, pp. 326, 327)
The confirmatory bias denotes the misinterpretation of ambiguous information, as evidence that confirms an initial opinion.

More importantly, it has been determined that an agent with a confirmatory bias habitually believes in hypotheses that are wrong, which at the same time, represents an opportunity for an observer to take advantage. Very often, private and public agents use the confirmatory bias to shape or strength wrong ideas.

So, although people show concerns for their privacy and crave for better control of the information, the extent to which people know how their privacy is being protected tends to be more limited, and it is often subject to intentionally provoked biases. Indeed, even while there is a general distrust of the public in the activities of data processing, the perception of people in this regard is frequently inaccurate.

There are no few examples of corporate power and media coverage diminishing privacy scandals, or supporting wrong ideas by implying that technology companies are strongly protecting the privacy of their users.

A very recent example is the dispute between Apple and the FBI. Apple denied the requirement made by the FBI to create a backdoor and, therefore, unlock an IPhone belonging to an alleged terrorist, arguing the defense of civil liberties and the protection of people’s privacy. While this refusal of Apple has been praised as a strong protection of the users’ privacy, it should not be forgotten that it has also served as an effective advertisement for the IPhone’s security and encryption. Moreover, Apple’s strong stand for security and privacy has signified great economic benefits for the company by providing successful access to markets like China, where people is increasingly concerned about state surveillance.

---

149 (Cartwright, 2011, p. 177)
150 (Rabin & Schrag, 1999, p. 38)
151 (Rabin & Schrag, 1999, p. 38)
152 (Staben, 2012)
153 (Kharpal, 2016)
154 (MacGregor, 2016)
155 (Grossman, 2016)
156 (Benner, 2016)
Other technology companies have crafted their media image in similar ways. Facebook’s Kathy H. Chan stated: “our philosophy is that people own their information and control who they share it with.” In the same way, Google's Eric Schmidt stated: “(M)y interpretation is that there is concern that we might be misusing this data and we're not telling you [about it], which I assure you is not the case. We're very committed to telling you what we do.”

In this context, is it ironic that according to the NSA, these three companies were aware and gave access to people’s data in the activities of mass surveillance performed within the PRISM program.

Moreover, other factors that create confirmatory bias in the data processing activity have been recognized. For example, Julian Staben argues that consumers are used to have protective warranties and cancellation policies in commercial purchases, which lead them to assume that the same protection applies to privacy policies.

Arguably, the creation of a confirmatory bias using the media and other means to promote a fake perception of protection of people’s privacy, along with the other behavioral phenomena already analyzed, have helped in the creation of an uninformed user.

A confirmatory bias may be used in a positive way of empowerment of data subjects, in the sense that under appropriate conditions and with enough information, the data subjects may be more critical in their perception of the commercialization of data and, therefore, be more careful in the disposition of such data.

5 Making a responsible data subject: Applying behavioral economics to create informed consent:

As it is clear from the previous lines, the aim of this work is to defend the consent as a proper mechanism for the protection of the right to privacy, on the grounds that the concept of consent has the potential to create control of the information of the data subjects.

157 (Chan, 2009)
158 (Grabham, 2013)
159 (Kleinman, 2016)
160 (Staben, 2012)
The models of behavioral economics previously mentioned are crafted after experimental results that have evidenced that certain economic models, based on ideal behavior, do not correspond to reality. Instead, the experiments have discovered that the actions of people can be more counterintuitive. In the application of these models to the data privacy field, certain conclusions and proposals can arise. The following lines contain a brief summary which will be followed by an exposition of these proposals.

So far, this work has shown that in the current model of data processing, the way in which the information is provided has not been adequate, because a complete understanding of the privacy terms and conditions is costly and impractical for the data subjects. This situation has arguably created a phenomenon of bounded reality, where the acceptance of privacy terms has lost most of its importance, and therefore, has become an automatic response. The same informational issue has made the data subjects unaware of the consequences of providing the data.

As expressed before, the phenomenon of “loss aversion” applied to the field of data protection, can be used in a way that shapes behavior, oriented to a more conscious and responsible decision-making. The fact that people tend to give a higher value to the losses in a transaction, and that people tend to stick with the gains they already have, may become an interesting tool to make the users more jealous of their information. Furthermore, the phenomenon of confirmatory bias seems very often to be grounded on informational problems, where people relies on fake assumptions.

Therefore, it seems that the analysis of these issues of bounded reality, loss aversion and confirmatory biases from the data privacy point of view, must lead to a proposal that creates a more sophisticated user. This purpose may be achieved by reconsidering the mechanism and the way in which the information of the data processing is being provided. This implies, from one part, to consider the content that it is being transmitted to the users, by making it relevant and user-friendly. Additionally, and to encourage a sophisticated user, this information should be provided in a unified and easily understandable and manageable way.

Moreover, the phenomenon of time inconsistency also shows that providing information by itself may not completely discourage a bounded reality decision-making. In practice, users will take quick automatic decisions lured by the immediate reward of an online service. Indeed, the phenomenon of time inconsistency may leave the sole provision of information as a useless
mechanism, in the sense that users prefer to assume certain costs, such as allowing access to data, in exchange for an immediate reward.

In the same line, the phenomenon of bargaining impasse cannot rely solely on the provision of information. As the bargaining impasse implies that what the users consider fair is conditioned to the benefits that the person may be receiving, this requires, not only to provide better information, but also to create a value-oriented approach. In this way, assigning a value to the data creates a real possibility of bargaining, contrary to the current unilateral model, oriented to benefit companies' interests exclusively.

In this sense, the following proposal, besides of relying in a better way of providing information in a unified and less-costly system, trusts that a value approach, where the users are able the quantify the value of the data and compare it with the service that is being offered in exchange, may create a better and more controlled scenario for users.

Taking this into account, the following sections will include a proposal of a model of data management from the users’ perspective. On the first place, it is analyzed if there are other methods to provide legal information to the users, in a way that allows better understanding. Moreover, considering the difficulties to create an informed data subject in a fragmentary scenario, the proposal envisages the need for creating a system that contains unified information of the data circulating online of the data subject, which may be boosted with the help of architectural decisions, or “code.” Finally, understanding the need for a more involved user and recognizing the need for awareness of said user in relation to the costs and rewards of the data exchange, it will be analyzed the possibility of implementing a model based on the value of the data.

5.1 Providing data processing information:

Arguably, the first issue that must be tackled is the quality and type of information that it is being provided to the users. Currently, the way in which the information of data processing is being provided is simply impractical and raises several issues for the users.

This impracticability is showed by several examples, such as the experiment performed by the Norwegian Consumer Council mentioned in Section 2.1. More specifically, Facebook is a good
example of this impracticability, since the data and cookies policies of the service amount to more than 4000 words, not including the Terms of Service, which sum other 4000\textsuperscript{161}.

In this scenario, it is evident that one of the main issues in the current model of data processing is to assume that an actual informed consent can be expected from the data subjects, in the way in which the information of the data processing is currently being provided.

According to the GDPR, there is a substantial amount of information that must be provided to the data subjects. Mainly, Article 13 contains such requirement, which includes the identity of the controller, purpose of the processing, the identity of the recipients, among others. Article 14 includes the information that must be provided if the data has not been obtained directly from the data subject.

Nevertheless, the way in which this information has been so far provided is not user friendly and, mainly, does not comply with its purpose, which is to properly inform the users on the basis of the principles of transparency (Article 5(a)) and Article 12(1) of the GDPR), and to create an informed user that can responsible provide consent.

But providing information for the data processing does not have to be this costly. In this line of thought, an example of providing legal information to a broad public is the Human Readable layer of the Creative Commons license. This tool was crafted with the understanding that most creators of content may not have a legal background, and therefore, require a more suitable set of information. Indeed, Creative Commons explains the purpose of the Human Readable in the following way:

\textit{(...) since most creators, educators, and scientists are not in fact lawyers, we also make the licenses available in a format that normal people can read — the Commons Deed (also known as the “human readable” version of the license)\textsuperscript{162}.}

Creative Commons managed to summarized difficult copyright concepts in user-friendly images. Concepts of copyright rules, such as the right to communicate, distribute or reproduce a work, the

\textsuperscript{161} (Facebook, 2015) \textsuperscript{162} (Creative Commons, s.f.)
attrition of moral rights, and other legal concepts, are contained in figures that do not require specialized knowledge.

In terms of privacy, some efforts have been made to provide better information to the users. In Germany, Wikimarx\textsuperscript{163} highlights the most critical or important provisions in the terms of service, although it requires a diligent and concerned user.

It is certainly valuable to recognize that, in most cases, the receivers of legal information online, especially in the field of data privacy, are not lawyers. In this sense, it is self-evident that relying on difficult and long privacy policies to prove the informed consent of a user is not an accurate way to create control.

In this sense, the way in which the information is provided should be reconsidered. The creation of a user-friendly method, such as the one used in Creative Commons is an interesting approach that should be considered in the data privacy scenario.

5.2 Unifying the information:

The practical problems that arise from the huge amount of information that the users are supposed to read should not be undermined. Even if the privacy terms and conditions of a service are provided in a user-friendly way, the disparities with the terms and conditions of other services, and the difficulties of understanding their differences will arguably not encourage users to take more responsible decisions. In this sense, the possibility of creating a unified system for data management may be a viable proposal to encourage control.

The idea of creating a unified system for the management of data is not necessarily a novelty. The FTC Commissioner Julie Brill created an interesting initiative called “Reclaim your Name,” by which she encouraged data brokers to create a consumer-friendly online service that would give access to the information that data brokers have of them\textsuperscript{164}.

\textsuperscript{163} (Wikimarx, s.f.)
\textsuperscript{164} (Brill, 2013)
Moreover, Data Management Platforms (DMP) have emerged during the last years, offered by companies like Oracle or Adobe\textsuperscript{165}. These platforms store data which, after a process of analysis, provides useful information for businesses, mainly profiles for targeted online ads\textsuperscript{166}. The DMPs, although mainly used for companies in the monetization of data, can be used as models of data management for users.

In this line of thought, startups like Datacoup have started the path of creating a value-oriented platform and marketplace for the users to sell their data for a fixed amount per month\textsuperscript{167}. The company Citizen Me provides a similar service for consumers with the possibility of earning cash or donating data to charity\textsuperscript{168}. Although the payment of a small amount of money in exchange of the data of all the social networks of the users is still far from an actual management and marketplace of data, the approximation to control of the data subject is certainly greater than before, as it provides the possibility for the data subject to not only manage unified sets of information but also to make this information a valuable good.

Eventually, a better-controlled scenario of a unified data management model may include other possibilities of control different than the sole possibility of selling the data as a whole. For example, in order to build trust in the user, a unified system should create standard privacy policies oriented to data processors and controllers. Eventually, a unified system may provide the user with tracking tools that identify the current controllers and processors of the data, or mechanisms that allow choosing the frequency and type of intrusiveness of advertisement.

Moreover, the emergence of platforms that are already implementing data management systems with a user-oriented approach\textsuperscript{169} shows the potential of the use of a “code” approach in the implementation of data policies.

\textsuperscript{165} More information about the Data Management Platforms of Oracle and Adobe can be found in the following links:
(Oracle, s.f.)
(Adobe, s.f.)
\textsuperscript{166} (Marshall, 2014)
\textsuperscript{167} For more information about Datacoup, see:
(Datacoup, s.f.)
\textsuperscript{168} For more information about Citizen Me, see:
(Citizen Me, s.f.)
\textsuperscript{169} (Simonite, 2014)
The objective of this section is not to create a detailed proposal in this matter, but to introduce a possible solution to the fragmentation of data management and information. In this sense, although it is not the focus of this work, it should be briefly recognized the importance of “code” in the role of regulating data processing.

“Code” can be broadly understood as the architecture of information of technologies that includes hardware and software. It is a recognized principle now that said architectural, and design choices have the capability of imposing rules on the participants of cyberspace, as a type of regulation, also called Lex Informatica. In other words, technological capabilities and system designs create rules for the users. As correctly stated by Langdon Winner, in deliberate or inadvertently ways “(...) the things we called “technologies” are ways of building order in our world.”

Lessig finds in “code” the new regulator in the online scenario. Nevertheless, code is subject to change under the influence of economic interests: “This regulator is code -- the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced (...) Unregulability is a function of code, but the code can change (...) Commerce is building these other architectures (...)”

The implementation of “Code” tends to be a self-regulatory response to unregulated scenarios. What it is clear is that in the online scenario, the difficulties of state enforcement seem to make necessary the use of self-regulatory mechanisms, as they present advantages in efficiency, flexibility, and cost. More importantly, the recognition of “code” as a paramount tool to shape behavior online, is also a recognition that in the online scenario it is impossible to simply rely on legislative and centralized measures, and that the role of private actors must be taken into account.

---

170 (Kesan & Shah, 2003-2004, pp. 279, 281)
171 (Reidenberg, 1998, p. 554)
172 (Reidenberg, 1998, p. 554)
173 (Winner, 1980, p. 128)
174 (Lessig, 2000)
175 (Koops, et al., 2006, p. 123)
5.3 A value-oriented model of data management:

5.3.1 How valuable is the data?:

There is generalized idea that the most common services provided online are free of charge. In reality, these services are profiting with the data gathered from the data subjects. Indeed, corporations are increasingly treating information as a commodity\(^{176}\), as there is a commercial exchange of value, where the internet service provider offers a service in exchange for data and attention\(^ {177}\).

In this sense, it is interesting to notice that on 2015, Facebook, with 1.59 billion subscribers, made approximately 9 to 13 dollars per user\(^ {178}\). In the medical field, it is estimated that the transfer of data will be worth more than 10 billion dollars by 2020\(^ {179}\).

The approximation of data as a valuable good is mostly discussed in the enterprise scenario. Indeed, so far, most analyses focus in considering the benefits for big companies in the technological market to treat data as a “natural resource.”\(^ {180}\) In this scenario, issues like antitrust have been analyzed when the value of the data and the intensive and disproportionate mining of said data can be assimilated to charging high prices\(^ {181}\). Moreover, the emergence of big data has allowed companies like Google, Apple and Amazon to offer bank-like services, all possible due to the enormous databases and a so far unreachable understanding of the consumer’s behavior\(^ {182}\).

This enterprise-oriented approach, which conspicuously recognizes the economic importance of data, not only disregards the possibility of individuals to dispose of their data but, on the contrary, aims to provide tools to monetize the data of the users for the exclusive benefit of companies\(^ {183}\).

---

176 (Victor, 2013, p. 517)
177 (Hasty, 2014-2015, pp. 297, 307, 313)
178 (King, 2016)
See also:
(Market Watch, 2016)
179 (Manyika, 2011)
180 (Deutscher, 2013)
181 (Cooper, 2013, p. 1131)
182 (Packin & Lev-Aretz, 2016, p. 1216)
183 (Twogood, 2014)
The discussion of providing value to the data in benefit of the users lags behind in the academic field and is almost inexistent in practice. This enterprise-oriented approach and the general understanding in businesses of data as a valuable good, not only contradicts the social perception but almost completely excludes the users from real economic benefits.

5.3.2 What do we get with providing value?:

This work believes that there are several advantages in the approach of providing value to the data in benefit of the users. From a competition point of view, the value-oriented approach provides better tools for controlling the activity of data processing. Indeed, Andrew Hasting notices that “a value approach may be more efficient in providing proves of deceptive practices where the agencies would be able to compare the value of the service in comparison with the “value” of the data provided in exchange, furtherly analyzing an unfair unbalance\(^\text{184}\). In other words, assigning value to the data arguably creates more objective basis to identify the abusive market behavior of technology companies.

In the same way, the value approach is clearly market-oriented. Thus it can have beneficial situations for consumers. Companies will be encouraged to provide better and more competitive services, contrary to the current scenario, where users download products and use services without necessarily considering their quality.

But more importantly for the behavioral-oriented approach of this work is the awareness that the value-oriented approach may create in the data subjects. It is undeniable that for most users, there is a lack of understanding of the flow of personal data and the ways in which this flow can be controlled\(^\text{185}\). This phenomenon has been mainly grounded on the unawareness of legislation and the acquaintance of the private and public actors, but has, so far, not taken into consideration the user’s perspective and actions.

The behavioral economics situations previously analyzed are benefited with a value-oriented approach. The phenomena of bounded reality and time inconsistency, where data subjects accept privacy limitations in an automatic way and expect an immediate reward, and the issue of “loss

\(^{184}\) (Hasty, 2014-2015, p. 318)

\(^{185}\) (Hasty, 2014-2015, p. 302)
aversion,” where users give more weight to the losses and, therefore, stick to their possessions, are all strongly connected. Indeed, tackling these issues as a whole may be done by relying on the awareness of the value of the data and the possibility of disposing of it, which makes the users mindful of the loss that implies a transaction, and leads them to give more weight to the loss of data than to the reward\textsuperscript{186}.

In the same way, the loss aversion derives in a more protective use of the self-serving bias. The bias of considering something fair when the outcome represents a benefit for the person\textsuperscript{187}, requires, also, an awareness of the value of the data, and the possibility of disposing of it. Furthermore, the bargaining impasse, where users believe in the fairness of their position in a transaction, certainly requires something to be bargained.

Related to the previous lines, another capital reason to support the value approach is the awareness of the users in relation to the degree of sensitivity of the data that it is being processed. Both the DPD and the GDPR include fairly protective provisions on the processing of sensitive data that reveals \textit{“ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.”}\textsuperscript{188} This restriction, nonetheless, is not always effective, as the processing of sensitive personal data may not always be evident. For example, the Passenger Name Record used by airlines often requires details of health conditions or meal preferences of the passengers which reveal, in turn, sensitive information of medical and religious nature of the travelers\textsuperscript{189}. In the same way, mortgage brokers use cookies and tracking tools that, after a process of analysis, can reveal the ethnic origin of a potential client\textsuperscript{190}.

The extent to which the provision of user-friendly information and the implementation of a value-oriented approach will protect the users against the processing of sensitive or potentially sensitive data is unknown. Nevertheless, it is valuable for a data subject to be aware, both of the potential

\textsuperscript{186} (Tversky & Kahneman, 1991, p. 1038)
\textsuperscript{187} (Babcock & Loewenstein, 2004, p. 326)
\textsuperscript{188} DPD Article 8; GDPR, Article 9.
\textsuperscript{189} (Enerstvedt, 2014, p. 27)
\textsuperscript{190} (Gangadhara, 2014)
of certain data to reveal sensitive information, and to be able to dispose of it at his will. This possibility is currently inexistent.

5.3.3 Value vs. Property:

Several theoretical approaches have tried to change the perspective of the data protection model to orient it toward a right to property of the data subject. Indeed, Professor Lessig states that “(T)he laws of property are one such regime. If individuals can be given the rights to control their data, or more precisely, if those who would use data had first to secure the right to use it, then a negotiation could occur over whether, and how much, data should be used”\textsuperscript{191}.

It is interesting to notice that critics of this model are grounded on the dangers of allowing consumers to treat their data as commodities, without being properly informed and having information disparities with the processors\textsuperscript{192}. The current state of technological developments, with the acquaintance of legislative rules, already did the job of putting the data subjects in this situation, with or without their knowledge.

Nevertheless, and although implementing a right to property of the data seems to bring control to the data subject, the whole concept of property lays on nebulosity and theoretical difficulties marked by endless conceptual disputes (is property an interest or a dominion of a thing?\textsuperscript{193}).

The classification of the type of data that may be subject to property may also present different problems. Indeed, several authors, especially in the medical field, have acknowledged the importance of certain types of data to be part of comprehensive databases for public health and safety\textsuperscript{194}. The conceptual issues of propertize data would require a throughout classification, which may provide weak protection for certain types of data or too strong protection for other.

Moreover, the recognition of the data subject as the owner of the data may have the same ineffectiveness that comes with the recognition of the right to informational self-determination. As stated by Professor Barbara J. Evans, the recognition of property does not necessarily imply legal property protection, as “(L)aw recognizes that there are many situations where consensual

\textsuperscript{191} (Lessig, 1998, p. 17)
\textsuperscript{192} (Victor, 2013, p. 518)
\textsuperscript{193} (Victor, 2013, p. 518)
\textsuperscript{194} (Evans, 2011, p. 88)
transactions cannot be relied on as a way of ordering an owner’s relations with the larger community.\textsuperscript{195}

Some authors even consider that the new GDPR creates a right to property in the data, in the sense that consent constitutes the most important ground for the processing of data and that the right to be forgotten provides further control\textsuperscript{196}. Nevertheless, relying on this legal recognition to consider that the data subjects are currently in control of their data, means to deny a self-evident reality that shows that this is not the case. Therefore, it seems that the recognition of the right to property without proper tools for achieving this end, is, as with the right to informational self-determination, nothing more than a rhetoric acknowledgment.

Moreover, the model of property of data, for some writers, requires the implementation of a highly regulated market\textsuperscript{197}, which requires, at the same time, a better suited but currently inexistent online context. Issues on the like of territoriality make a model based on property impractical and hard to implement, due to the fact that, despite certain and significant convergences, legal disparities on national laws in relation to outsourcing, data mining, or information security\textsuperscript{198} make a global implementation of policies very difficult.

6 Conclusion:

In 1998, Lawrence Lessig prophesied that “we are entering an age when privacy in any sense of that term will be fundamentally altered: An age when the extent of the monitored, and the reach of searchable, is far greater than any we have known. We can choose to let this change occur. Or we can choose to do something in response.”\textsuperscript{199}

Sadly, it seems that in the current online scenario, this active suggestion of Lessing, almost 20 years old, has been disregarded or put aside. Nevertheless, the concerns raised by monitoring activities in the field of privacy are more present than ever. Optimistically, it is not too late to accept Lessig’s proposal, look outside the box, and seek for a better solution.

\textsuperscript{195} (Evans, 2011, p. 88)
\textsuperscript{196} (Victor, 2013, p. 523)
\textsuperscript{197} (Victor, 2013, p. 519)
\textsuperscript{198} (Gunasekara, 2006, p. 375)
\textsuperscript{199} (Lessig, 1998, p. 2)
It is not too late to make the normal user aware of these challenges. What this work has shown is that the people’s perception in relation to data privacy seems to maintain an ideal of control that must not be disregarded, even if the reality of the online scenario diminishes this fact.

Alan F. Westin, stated that "(T)he modern totalitarian state relies, to varying degrees, on secrecy for the regime and full surveillance and disclosure for all other groups. Both fascist and communist literature have attacked the idea of privacy as "immoral," "antisocial," and "part of the cult of individualism."200 This work agrees with this vision and regards the current state of affairs as a dangerous one, where surveillance maintains its capital importance, delegitimated by unnecessary intrusions into normal people’s privacy.

Both Lessig and Westin should be brought to the present, by recognizing that data and information are paramount and necessary assets for the development of technology but that, as accurately stated by Lessig, a response advocating for privacy is required in order to avoid what Westin identifies as the disclosure and surveillance that entail and lead to totalitarian societies.

This work believes that such response requires better ways of empowerment for the users. Such empowerment, which on paper seems to be present in the GDPR with the tool of consent, right to be forgotten, among others, has proved ineffective.

This situation, greatly influenced by the lobby and economic objectives of both legislators and businesses, arguably lays on the lack of consideration of other scenarios and perspectives. The proposal of this work is to consider such alternative perspectives, by providing mechanisms that empower the data subjects. The field of behavioral economics, which takes into account psychological considerations, can be a valuable tool for this purpose. More importantly, this change to a behavioral-oriented perspective has, as the main objective, to shape a desired behavior on the users, in the sense of creating a truly responsible data subject that can take informed decisions over the data.

The analysis of the phenomena that affect people’s behavior shows unexpected outcomes that, at the same time, require the implementation of different tools. This work supports the idea that a

200 (Westing, 1966, p. 1018)
better and more user-friendly way to provide information can be a strong mechanism to empower the users.

Nevertheless, behavioral situations show that this may not be enough. Thus, this work proposes a unified data management system, which may be created as an architectural choice in the way of “code.” Such system must provide the information required for the user, create a unified way of managing all data, and, finally, create value for the data as a real marketplace. The aim of these tools is to encourage actual involvement and an economic benefit for the user.

A model that provides a tangible value to the data should encourage the data subject to consciously choose the purpose of such data. For this to happen, the data subject must be fully aware of the type of data, the purpose of the processing, and the retribution received for the processing.

The proposal of this work, although specifically focused on creating tools of control, does not aim as far as to create a property right on the data subjects, considering that this measure, in itself, is not enough. In other words, the approach of this proposal seeks to be practical, relying on the need of control of the data subjects, based on the privacy values that drive the data protection field, and the fact that the data, in reality, acquired the characteristics of a commodity.

In any case, the previous works should be understood as an effort to change the direction in which the activities of data processing have been so far oriented. The new direction that the current online scenario demands must be oriented to the benefit of data subjects. This effort implies recognizing the dangers of the unlimited data processing performed by companies and states and creating tools to face such dangers. Since it is clear that these tools require an active involvement of the data subject, the way to implement them must attain reality and be based on actual conduct and behavior of the users of the internet. In summary, the model here proposed seeks to find solutions in the reality, by facing the social perception and individual behavior and aiming for the respect of the fundamental right to privacy and the need of control of the users.
II. Bibliography:


privacy/244971/  
[Accessed 18 7 2016].


[Accessed 18 7 2016].

Available at: http://www.citizenme.com/  
[Accessed 18 7 2016].


Available at: https://creativecommons.org/share-your-work/licensing-considerations/  
[Accessed 18 7 2016].

Available at: https://datacoup.com/  
[Accessed 18 7 2016].

Available at: http://www.privacysurgeon.org/blog/incision/why-the-idea-of-consent-for-data-
processing-is-becoming-meaningless-and-dangerous/
[Accessed 17 7 2016].

Available at: https://www.justice.gov/archive/ll/highlights.htm
[Accessed 26 7 2016].

Available at: http://siliconangle.com/blog/2013/03/11/ibms-ceo-says-big-data-is-like-oil-enterprises-need-help-extracting-the-value
[Accessed 18 7 2016].


Available at: https://edri.org/data-protection-lobbyotomy-part-1-influencing-the-dutch-government/
[Accessed 17 7 2016].


51) Joined cases C-465/00, C-138/01 and C-139/01. Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk (2003) Court of Justice of the European Union.


processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Brussels: s.n.


106) Villas-Boas, A., 2015. I tried using an anonymous browser, and it was incredibly annoying. [Online]
Available at: http://www.techinsider.io/anonymous-web-browsing-is-impossible-2015-12
[Accessed 17 7 2016].


Available at: https://w3techs.com/technologies/details/ce-cookies/all/all
[Accessed 18 7 2016].


Available at: http://www.wikimarx.de/
[Accessed 8 9 2016].