#### POLICY PAPER ON COOKIES CONSENT REQUESTS:

### EXPERIMENTAL EVIDENCE OF PRIVACY BY DEFAULT AND DARK PATTERNS ON CONSUMER PRIVACY DECISION MAKING

The development and growth of data analysis and processing programs involving the use of big data tools have made it easier to search, link, and track personal information (Yeung, 2017). Consequently, internet users can be easily targeted through online identifiers provided by their devices, applications, and other tools. The activation of these identifiers enables users to leave traces that, when combined with unique identifiers and other data received by the servers, can be used to create profiles of an individual and identify them. Moreover, there is a risk of identifying an individual without establishing their civil identity but knowing the subject's activity and connecting various interactions with an individual. Accordingly, consumers are increasingly exposed to consciously or unconsciously submitting information in the digital world without necessarily knowing how and to what extent their data is collected, stored, and processed (Smit et al., 2014; The Behavioural Insights Team, 2019).

One of the main techniques to collect such data is the use of cookies on internet websites. Cookies are pieces of text used to retain information in web browsers to store and receive identifiers and other data on computers, phones, and other devices (Debusseré, 2005). According to this, the literature highlights that there will be different levels of exposure and risks to consumers' data depending on the scope and combination of cookies used. At the same time, the evidence shows the existence of a `privacy paradox' because most people declare that they are very concerned about their privacy, but their online behaviour differs from this concern. There is no single cause for this paradox; however, cognitive biases and the complexity of evaluating the impact of online decisions on privacy protection are among the reasons for this behavioural paradox (Kokolakis, 2017; Barth & D.T. de Jong, 2017).

Additionally, it is common for cookie consent agreements to display information in a manner that makes it difficult to understand its content, especially when the response is performed in a few seconds (Kulyk et al., 2018). Consequently, people tend to provide more information than they would consciously provide (Norberg et al., 2007; Spiekermann et al., 2001). For this reason, regulators should assess to what extent interfaces that consider the influence of these cognitive biases can facilitate or hinder people's decision-making in line with their privacy preferences (OECD, 2018).

Considering the above, the European regulation has implemented "privacy by default" as one of the main pillars of its General Data Protection Regulation (GDPR). According to this, those responsible for collecting and processing personal data must apply technical and organisational measures to ensure that, by default, only personal data is collected and processed when it is strictly necessary for the specific purposes of processing it. In line with the behavioural science literature, the European Regulation assumes that the choice architecture that minimise the risk of sharing unwanted



personal data is where the default option is to reject cookies that lead to the collection of their personal data and are not strictly necessary for the website. However, unlike the European experience, the current Chilean regulation has not included the principle of privacy by default yet. Nevertheless, a bill that modifies Law No. 19,628 on protecting private life is currently under discussion in Congress. It incorporates the duty to protect privacy by design and default, among other reforms.

Thus, considering the state of national regulation and the risks associated with the use of cookies in electronic commerce, SERNAC carried out a field experiment to evaluate options to inform and request the consent of consumers about using additional cookies during their internet browsing. This policy paper, prepared by a multidisciplinary team of SERNAC<sup>1</sup>, summarises the technical report published on our webpage (in Spanish only)<sup>2</sup>.

The policy paper is structured in five sections. The first section (I) summarises the main literature associated with people's behaviour in terms of privacy and online behaviour. The second section (II) introduces the results of an online survey on personal data and the use of cookies to diagnose the problems in the Chilean context. The third section (III) exposes the evaluation mechanism and describes the experimental design. Then, the main statistical results of the experiment (IV) are presented. Finally, the fifth (V) section gives conclusions and formulates a regulatory proposal according to the collected evidence.

#### **1. LITERATURE REVIEW**

**The Privacy Paradox.** The privacy paradox is the discrepancy between the expressed concern and users' actual behaviour. Thus, people claim to be very concerned about their privacy but do very little to protect their data (Kokolakis, 2017; Barth & DT DeJong, 2017). However, due to cognitive biases, heuristics, and bounded rationality, it is unclear how users autonomously consent to the conditions and potential consequences of exchanging their personal data when navigating online. Indeed, depending on the cookie settings defined by the Internet service provider, users could even transfer personal data to third parties without a clear knowledge or understanding of its consequences (Loewenstein et al., 2013). The risks of transferring this personal data are unclear or, at the very least, tough to assess (Grossklags & Acquisti, 2007). As a result, users will be more likely to make online decisions that are not fully aligned with their preferences in protecting their data.

**Default Options.** Thaler and Sunstein (2009) argue that in the presence of limited rationality and heuristics in people's decision-making on relevant issues, incorporating 'nudges' as a change in the default rules can help individuals in their

<sup>&</sup>lt;sup>1</sup> Andrés Pavón Mediano, Subdirector of Financial Consumption, MSc in Regulation, LSE, MSc in Public Policy, UCL; Francisca Rabanales Riera, Behavioural Economics Coordinator, MPA in Economic and Social Policy, LSE; Carol Luengo Miranda, Financial Economist Analyst, Master in Economics, UDEC; Gonzalo Vergara Araya, Privacy Data Coordinator, MSc in Regulation, LSE, LL.M en Law & Technology, University of California, Berkeley.

<sup>&</sup>lt;sup>2</sup> Accessible in the following link: <u>https://www.sernac.cl/portal/619/w3-article-64969.html</u>

decision-making process. According to this, several studies have shown that default options or preselected answers have a very significant impact on people's decisionmaking, since they tend to keep the option given by default and, therefore, their decision is influenced by the choice architecture predefined by the regulator or the industry (Samuelson & Zeckhauser, 1988). In this sense, default selections are a powerful tool to guide people's behaviour in a specific direction, preserving their freedom of decision (Sunstein, 2019). There are two common options on how to present defaults: opt-in and opt-out options. In the first scenario, people must perform an (active) action to accept or adhere to the options displayed, which means that by default, they have not subscribed to the choices presented. In the second, individuals must act to reject or deactivate something that is accepted or subscribed to by default. For this reason, in cases of cookie consent notices, the industry usually uses default options to encourage the acceptance of all cookies, while for rejecting them, users must go through different steps and disable them.

**Dark patterns.** There is not an established international definition for dark patterns, however, Harry Brignull started using the term in 2010 to describe "tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something". Over time, the international community has understood them as practices or techniques in websites or interfaces that steer, deceive, coerce, or manipulate consumers into making potentially harmful choices or choices that are not aligned with their preferences (Brignull, 2022; Mathur et al. 2019). Utz et al. (2019) showed that the widespread use of nudges - in the form of dark patterns - significantly influences users' privacy choices. Graßl et al. (2021) - through two experiments - showed that most of the participants accepted all cookies regardless of the type of dark pattern they faced, as opposed to bright patterns that encouraged the protection of their privacy. Consequently, the literature shows the relevance of evaluating the impact of the use of dark and bright patterns in the process of collecting cookies' consent.

### 2. SURVEY RESULTS

An online survey was carried out to assess people's knowledge of cookies, their online behaviour, preferences in personal data matters, and testing messages to be used in the experiment.

**Characterization of the sample.** A representative sample of consumers who made online claims and/or online queries to SERNAC during 2020 were invited to participate. There were 683 valid answers of which 53.44% of the participants identified as females and 45.1% as males. The participants were between 17 and 77 years old, being the age group 25-65 the one with the greatest participation rate. Likewise, consumers with different levels of education participated. In addition, 97.95% of participants stated a daily - or almost every day - use of the internet for personal use.

**Survey protocol.** People who received the invitation to participate in the study - and accepted the informed consent - answered two sections of the survey. Based on the study by McDonald & Cranor (2010) and Lancefield et al. (2011), the first section



assessed the level of concern about participants' personal data on the internet, the perception of sensitivity of this information, and their prior knowledge about cookies. The second section randomly divided the participants into four groups. Participants received a message that simulated what could appear on a website about the use and setting of cookies. This allowed us to directly evaluate the impact on participants' willingness to accept or not to accept cookies, the users' level of information about their privacy options, the ease of understanding messages, and the time they would be willing to spend reading a similar message in a real context.

**Results.** The survey results indicated that the privacy paradox exists by showing the discrepancy between the expressed concern and their stated behaviour - 53.9% of the respondents indicated that they were "extremely concerned" that their personal data could be collected without their consent. However, only 3.22% of them stated that they always read the privacy policies of a website (Figure 1).



Likewise, the results showed that 34.11% of the participants declared that they do not understand what cookies are and what they do, while 2.34% had not even heard of them before. These differences are particularly important when analysing educational attainment and age. There is a positive correlation between knowledge of cookies and education levels and between knowledge of cookies and age. Additionally, participants declared whether they agreed or disagreed with statements related to the use and protection of their data. In this context, 28.11% of participants agreed to provide personal information if it would save them time on their next visit to the website. On the other hand, 22.11% of the participants stated that they agreed with the statement, "I am willing to give my personal information if that helps websites offer me discounts or relevant offers." (Figure 2).



Figure 2: Willingness to provide personal information in some scenarios

I am willing to give my personal information if:

Regarding users' concerns during browsing on the internet, 82.28% of them indicated that they agree or totally agree that they are concerned that web pages collect their personal data. In addition, 81.55% agree or totally agree with the statement, "I would monitor what I do on the Internet more carefully if I knew that web pages were collecting my personal data". On the other hand, 38.51% of people indicated that they disagree or totally disagree with the statement "I am clear about the type of personal data that web pages can collect from me". Finally, the participants answered that, on average, the most sensitive information for them is their name, RUT (Chilean's personal identifier), and address, followed by their financial information and genetic and/or biometric data to uniquely identify a person, such as fingerprints.

The second section of the survey randomly assigned participants to four formats of cookie consent requests<sup>3</sup>. The methodological design allowed obtaining evidence of the impact of each of the messages tested on different aspects. These formats were designed to test two main hypotheses: (i) the type of information included in cookie consent requests have an impact on consumers' decision<sup>4</sup>; and (ii) information salience can attract the attention of readers increasing content comprehension. Appendix 1 exposes the four messages.

The results show that designs with information about what cookies are and what they do achieve the highest percentage of declared rejection of additional cookies and the

<sup>&</sup>lt;sup>3</sup> Random assignment by blocks considering age and level of concern.

<sup>&</sup>lt;sup>4</sup> For this, we designed messages considering information about what cookies are and do, information about consumers' privacy rights and social norms on privacy behaviour

level of understanding about them (Figure 3). In addition, all designs increased people's level of knowledge. However, the "Comprehension salience" treatment obtained the highest percentage of people who declared to be more informed about their privacy options after reading this information. Based on these results, it is recommended that the field experiment considers a message that explains simply and clearly what cookies are and what they do in the consent request for the use of cookies not including information regarding people's privacy right or information about the behaviour of others.



### Figure 3: Willingness to accept or reject cookies by message

### 3. METHODOLOGY OF THE EXPERIMENT

Based on the literature review, the online survey results, and a review of Chilean, European and American websites, 4 areas of action were selected to generate the prototypes for the experimental phase:

- (i) A formal request of the consent for the use of additional cookies;
- (ii) Incorporating information on the use and purpose of cookies;
- (iii) Modifying default options (opt-in or opt-out); and
- (iv) Adding aesthetic manipulations that highlight options that motivate or discourage decisions that restrict the acceptance of additional cookies (dark and bright patterns).

The field experiment was carried out on SERNAC's webpage with 70,208 unique users. For this, five prototypes of different personal data protection standards were



designed and tested, in contrast to a message with a low standard used by national businesses. The content and format of the cookie consent prototypes tested on the SERNAC website are detailed below.

 "Strong dark Pattern" (Control group): The message only informs about the use of cookies on the website while not expressing a formal request for consent. The only option to reply is the "accept all" button, and it does not inform the option to alter the configuration. In case of wanting to change it, they must enter the privacy policy through the link included in the text (Figure 4). Once, inside the privacy policy, at the end of its text, the option for change cookies was given, which by default have an opt-out format.





2. "Dark pattern" (Treatment 1): It provides a summary of what strictly necessary cookies are and requests consent for using additional cookies. Users have the option of managing or accepting additional cookies through the "Cookie settings" and "Accept additional cookies" buttons (Figure 5). In the case of selecting "Cookie settings" users saw the definition of each of the cookies in an opt-out default format.

Cons	entimiento	
Nues Utiliza servic visitas	t <b>ro uso de cookies</b> imos cookies "técnicas" ios del sitio web, y cook s y usos del sitio web. Pa	que permiten ejecutar funciones, opciones y ies de "análisis" para generar estadísticas sobre las ara utilizar cookies adicionales de personalización, miento requerimes eu consentimiento
gestió	n de anúncios y perfilai	mento requermos su consentimiento.

Figure 5: Treatment "dark pattern"

3. "Dark pattern with more information" (Treatment 2): It gives the same reply option as treatment 1 but expands the content of the initial message, explaining what cookies are and what they do (Figure 6). Additionally, in the case of selecting the "Cookie settings" option, users were given the definition of each of the cookies in an opt-in default format.



4. "Bright pattern with more information" (Treatment 3): It has the same message shown in the previous case, but the response options change to "Cookie settings" and "Reject additional cookies". If users select "Cookie settings", a definition of each of the cookies in an opt-in default format was given (Figure 7).

Figure 6: Treatment "dark pattern with more information"

# Figure 7: Treatment "bright pattern with more information"



- **5.** "**Opt-in**" (**Treatment 4**): It gives full information and the option to manage cookie settings in a unique message, so users can select the additional cookies they want to activate (Figure 8).
- **6.** "**Opt-out**" (**Treatment 5**): It is the same message and format than the previous case, but all additional cookies are selected. Therefore, users must deactivate them to reject all additional cookies (Figure 9).

#### 4. RESULTS

Seventy-two thousand and two hundred and eight (72,208) valid unique users visited SERNAC's website between January 8 and 22, 2022. Once the users entered the site www.sernac.cl, they were randomly assigned to one of the experimental conditions, which determined the message or pop-up they would observe in their first interaction with the website. Depending on the assigned message and the user's decisions, the participants could interact with a maximum of three pop-ups.



### Figure 8: Treatment "opt-in"

archivos de texto que los sitios web colocan en su dispositivo a. Usted debe saber que algunas cookies pueden recopilar y ación como su dirección IP, ubicación y otros datos personales, r compartidos con terceros. e cookies as ookies son necesarias para la navegación del sitio web y r elementos de seguridad durante la navegación. La información tada por estas cookies se encuentra anonimizada y es de carácter tico. is ookies permiten cuantificar el número de usuarios/as y es dentro del sitio web, para medir cómo se utiliza el sitio web. rmación recolectada por estas cookies se encuentra anonimizada carácter estadístico.
archivos de texto que los sitios web colocan en su dispositivo a. Usted debe saber que algunas cookies pueden recopilar y ación como su dirección IP, ubicación y otros datos personales, r compartidos con terceros. a cookies as pokies son necesarias para la navegación del sitio web y r elementos de seguridad durante la navegación. La información tada por estas cookies se encuentra anonimizada y es de carácter tico. is poskies permiten cuantificar el número de usuarios/as y es dentro del sitio web, para medir cómo se utiliza el sitio web. rmación recolectada por estas cookies se encuentra anonimizada carácter estadístico.
a cookies as ookies son necesarias para la navegación del sitio web y r elementos de seguridad durante la navegación. La información itada por estas cookies se encuentra anonimizada y es de carácter tico. is ookies permiten cuantificar el número de usuarios/as y es dentro del sitio web, para medir cómo se utiliza el sitio web. rmación recolectada por estas cookies se encuentra anonimizada carácter estadístico.
as ookies son necesarias para la navegación del sitio web y r elementos de seguridad durante la navegación. La información tada por estas cookies se encuentra anonimizada y es de carácter tico. is ookies permiten cuantificar el número de usuarios/as y es dentro del sitio web, para medir cómo se utiliza el sitio web. mación recolectada por estas cookies se encuentra anonimizada carácter estadístico.
is ookies permiten <b>cuantificar el número de usuarios/as y</b> es dentro del sitio web, para medir cômo se utiliza el sitio web. rnación recolectada por estas cookies se encuentra anonimizada craétere restadístico.
consentimiento para utilizar las siguientes cookies adicionales:
nalización ookies permiten acceder al sitio web con características finidas por el responsable de este sitio web, como por ejemplo el , el tipo de navegador a través del cual se accede al servicio, su rración regional, etc.
n de anuncios ookies permiten gestionar el funcionamiento de los espacios e iones de anuncios en el sitio web, sin tener en cuenta un perfil fico del usuario/a.
miento ockies permiten almacenar y rastrear los hábitos de ación del usuario/a para desarrollar su perfil específico y rle anuncios en función de su comportamiento en línea.
r c d a c citit a c citit a c

Figure 9: Treatment "opt-out

#### 4.1. Salience of managing cookies settings

Figure 10 shows that 98.57% of the participants assigned to the "strong dark pattern" design - commonly used by the national industry - accept additional cookies in the first message displayed. Only 1.43% clicked the link to the privacy policy to learn more about cookies and to be able to manage them. This is important to note because, in a scenario in which the industry uses messages like the one described here, the default option will determine users' level of additional cookies agreement.

The "dark pattern" treatment should (presumably) encourage the rejection of additional cookies because this design includes an express reference to the request of consent to use additional cookies and exposes more visibly the option to manage them. However, the results show that only 6.52% of the participants exposed to the "dark pattern" treatment enter to manage their options, increasing only 5 percentage points compared to the control group. Consequently, highlighting the dark pattern determines the result in both cases.



### 4.2. **Providing more information**

Many public policies regarding the protection of personal data use the technique of providing more information with the idea that people make better choices with new insights. The "dark pattern with more information" treatment sought to evaluate its efficacy. The results of the experiment indicate that 6.25% of the participants exposed to the "dark pattern" treatment selected the option to manage their cookies, and 5.52% did the same when receiving the "dark pattern with more information" treatment. Contrary to expectations, the provision of more information decreased the number of users who choose to manage their cookies in a context in which the presence of dark patterns is maintained. As a result, more than 90% of users maintained the default option of consenting additional cookies (Figure 11).



Figure 11: User's response in the first pop-up



### 4.3. Dark and Bright Patterns

When comparing experimental conditions with identical content but different aesthetic manipulations, the results show that 94.48% of the participants in the "dark pattern with more information" treatment accept all additional cookies, while 67.17% of the participants in the "bright pattern with more information" treatment choose to reject them. These results – in line with the literature - demonstrate the relevant impact that minor alterations have on users' privacy decisions (Figure 12). Consequently, when the pursued objective is to reduce the risk of accepting additional cookies, highlighting the option to reject additional cookies is an effective alternative.

Moreover, when analysing participants who choose the option to manage their cookies, those who received the treatment "bright pattern with more information" increase their likelihood of rejecting all additional cookies thanks to an opt-in default setting in the second pop-up. Therefore, 95.11% of users reject additional cookies when the design has a bright pattern in combination with an opt-in default setting (Figure 13).





### 4.4. The Impact of Default Options

Changing default options is an essential nudge in the literature and, given its application by the GDPR, its evaluation was especially relevant. Two cookie consent notices were tested with identical content but differing by showing additional cookies as selected (opt-out) or not selected (opt-in). In both cases, users could accept or reject additional cookies without entering a second pop-up to manage their cookie settings because the first pop-up included all the information and the settings options.

The study results show that 86.72% of the users exposed to the "opt-in" treatment maintained the default setting - rejecting the additional cookies presented to them - compared to only 5.60% of the users exposed to the "Opt-out" treatment. This



confirms that, in terms of cookie consent notices, the privacy by default determined by the industry or regulator will be decisive in the user's choice (Figure 14 and 15).



### 4.5. First privacy decision-making

Figure 16 shows users' choice in the first pop-up that they received for all prototypes tested in the experiment. This first analysis shows that it is highly likely that users will accept all additional cookies immediately. Indeed, more than 93% of users in the three experimental conditions that included a dark pattern accept all additional cookies. On the contrary, when the option to reject cookies in the first instance is highlighted, more than 60% of participants reject all additional cookies.

Moreover, results ratify the relevance of default options. The "Opt-in" treatment is the one that achieves the highest level of rejection of all additional cookies when considering the interaction with the first pop-up since 86.72% followed that option. On the contrary, when additional cookies are preselected by default (opt-out treatment), 93.43% of users accepted all additional cookies.



### 4.6. Second privacy decision-making: The aggregate effect

Notwithstanding the foregoing result, it is important to analyse the aggregate results of users' decisions when participants selected the option to manage their cookies. As Figure 17 shows, 95.11% of users reject the subscription of additional cookies when receiving the treatment "bright pattern with more information" with an opt-in setting in the second pop-up. Users who reject additional cookies in the first pop-up (67.17%) and users who enter to manage their cookies and keep the default option (rejection of additional cookies) explain this effect. Thus, the combination exceeds the rejection levels obtained by the "Opt-in" treatment in the first pop-up (86.72%).





#### Figure 17: Users' choice in both pop-ups

% users who subscribe or not cookies

#### 5. CONCLUSIONS AND PROPOSALS FOR REGULATORY IMPROVEMENT

The results indicate that two prototypes designed by SERNAC increased the probability of consumers rejecting all additional cookies by 94 and 86 percentage points. These effects are explained by (i) the aesthetic manipulation of consent requests highlighting options that induce consumers to reject additional cookies (bright pattern) and (ii) by an opt-in default privacy setting when requiring the consent of additional cookies to users. Specifically, the "bright pattern with more information" treatment in combination with an opt-in default setting increased the level of rejection of additional cookies by 94.3 percentage points compared to the control group or "strong dark pattern" design. Similarly, the "Opt-in" treatment also achieved a high rejection of additional cookies (86 percentage points).

On the other hand, all the designs that encourage the acceptance of cookies - through combinations of dark patterns and opt-out default settings – manage to nudge more than 90% of users into accepting additional cookies and, therefore, leaving their data more exposed online. This ratifies the central relevance of dark patterns and default privacy rules in the mechanisms to obtain consent for the use of cookies. Additionally, results also indicate that the mere use of cookie consent notices that incorporate links to the cookie policy of the website - as is currently the case with multiple national providers - is highly detrimental to users, when, by default, additional cookies are active (opt-out), since only 1.4% of users access the link that allows managing cookies.



Considering the different designs and results, the following lessons emerge to guide the definition of public policy on the matter:

- **Lesson 1:** Default options have a key impact on cookie consent decisions. Therefore, considering public policies that integrate the design by default will be more effective, as the GDPR has done in Europe.
- Lesson 2: Privacy settings through links in a text that lead to the privacy policy and in which the general acceptance of cookies is highlighted is harmful to users.
- **Lesson 3:** Highlighting the option to manage cookies through a button in the cookie consent notice and maintaining a dark pattern that encourages the acceptance of cookies is unlikely to reduce the risk of accepting additional cookies.
- Lesson 4: Simply providing more information about what cookies are and what they do does not lower the level of acceptance of additional cookies. The results indicate that the most relevant thing to consider is the default rule and the design format (dark/bright pattern) used by the website to request consent to the use of additional cookies.

**Proposal for regulatory improvement.** Considering the study results, SERNAC formulated a regulatory improvement proposal for consumers' online personal data protection. This proposal recommends that at the time of regulating the consent for the collection and processing of consumers' personal data it is important to have the following in mind:

- 1) **Principle of privacy by default (opt-in):** In line with the European standard, it is recommended that the Chilean regulation establish the principle of privacy by default so that an active manifestation of consent must be required from consumers to use any cookies that are not strictly necessary to operate the website. With this, it is possible to reduce the probability of unwanted acceptance of cookies that risk the collection of personal data. The foregoing is in line with the ongoing legislative debate for the reform of Law No. 19,628, on the protection of private life.
- 2) Use of bright patterns: Use aesthetic manipulations in favour of consumers using bright patterns, which facilitate the rejection of additional cookies. Contrarily, given their effects on the acceptance of additional cookies, the proliferation of dark patterns such as those used in this experiment is not recommended.
- 3) **Simple and clear language:** To publicise the use of cookies and their purpose, it is suggested to use language that consumers can understand without prior knowledge of technologies and cookies.
- 4) Inform the type of cookies and their purpose: A good practice is to provide information to consumers about the use and purpose of the cookies used on a site, as well as the time in which the data is stored (persistent cookies), and who will have access to the data collected (own or third-party cookies). This will be even more important when cookie consent messages begin to be implemented since these will be unknown to consumers.



Considering these lessons, the results of this experiment allow us to recommend two cookie consent notices that substantially increase the probability of rejecting cookies that are not strictly necessary for using a website.

The first cookie consent notice assumes that, in the first interaction with the user, consent to use additional cookies should be requested using a binary response with a bright pattern to reject additional cookies. Additionally, in the case of choosing the "setting cookies" option, an opt-in format must be in place, where the rejection of additional cookies is preselected by default (Figure 7). The second recommended cookie consent notice is one in which, in a single interaction with the website, the possibility of managing cookies is directly presented, but additional cookies are disabled by default (opt-in format) (Figure 8).



### 6. REFERENCES

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Brignull, H. (2022, March 23). Dark Patterns. https://www.darkpatterns.org/

- Debusseré, F. (2005). The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster? *International Journal of Law and Information Technology*, *13*(1), 70–97. <u>https://doi.org/10.1093/ijlit/eai003</u>
- Graßl, P. A. J., Schraffenberger, H. K., Zuiderveen Borgesius, F. J., & Buijzen, M. A. (2021). *Dark and bright patterns in cookie consent requests*.
- Grossklags, J., & Acquisti, A. (2007). What Can Behavioral Economics Teach Us about Privacy? En S. D. C. di Vimercati, S. Gritzalis, C. Lambrinoudakis, & A. Acquisti (Eds.), *Digital Privacy* (pp. 363-377). Auerbach Publications. <u>https://doi.org/10.1201/9781420052183.ch18</u>
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134. <u>https://doi.org/10.1016/j.cose.2015.07.002</u>
- Kulyk, O., Hilt, A., Gerber, N., & Volkamer, M. (2018). 'This Website Uses Cookies': Users' Perceptions and Reactions to the Cookie Disclaimer. *Proceedings 3rd European Workshop on Usable Security*. European Workshop on Usable Security, London, England. <u>https://doi.org/10.14722/eurousec.2018.23012</u>
- Lancefield, D., Ambler, M., Rauber, M., & Patel, R. (2011). *Research into consumer understanding and management of internet cookies and the potential impact of the EU Electronic Communications Framework*. PwC. <u>https://assets.publishing.service.gov.uk/government/uploads/system/uploads/</u> <u>attachment\_data/file/77641/PwC\_Internet\_Cookies\_final.pdf</u>
- Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1–32. <u>https://doi.org/10.1145/3359183</u>
- McDonald, A., & Cranor, L. F. (2010). *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising* (SSRN Scholarly Paper ID 1989092). Social Science Research Network. <u>https://papers.ssrn.com/abstract=1989092</u>
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. <u>https://doi.org/10.1111/j.1745-6606.2006.00070.x</u>
- OECD. (2018). *Improving online disclosures with behavioural insights* (OECD Digital Economy Papers No. 269; OECD Digital Economy Papers, Vol. 269). https://doi.org/10.1787/39026ff4-en
- Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal* of Risk and Uncertainty, 1(1), 7–59. <u>https://doi.org/10.1007/BF00055564</u>
- Smit, E. G., Van Noort, G., & Voorveld, H. A. M. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, 32, 15–22. <u>https://doi.org/10.1016/j.chb.2013.11.008</u>

- Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior. *Proceedings of the 3rd ACM Conference on Electronic Commerce*, 38–47. <u>https://doi.org/10.1145/501158.501163</u>
- Sunstein, C. R. (2019). Sludge and Ordeals. *Duke L.J. 1843*, 68. <u>https://scholarship.law.duke.edu/dlj/vol68/iss8/6</u>
- Thaler, R. H., & Sunstein, C. R. (2009) Nudge: Improving decisions about health, wealth, and happiness.
- The Behavioural Insights Team. (2019). *Improving consumer understanding of contractual terms and privacy policies: Evidence-based actions for businesses*. <u>https://www.bi.team/publications/improving-consumer-understanding-of-contractual-terms-and-privacy-policies-evidence-based-actions-for-businesses/</u>
- Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 973–990. https://doi.org/10.1145/3319535.3354212
- Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society, 20*(1), 118–136. <u>https://doi.org/10.1080/1369118X.2016.1186713</u>



#### 7. Appendix

**Appendix 1:** Designs for cookie consent requests tested on the survey

1. "Comprehension text" (control group): Based on the idea that more information would make people less likely to accept cookies. For this, it provides additional information about what cookies are and what they do as it is very common on European websites (Figure 18).

#### Figure 18: "Comprehension text" design

#### Consentimiento

#### ¿Qué son las cookies?

Las cookies son archivos de texto que permiten guardar y enviar información desde un navegador. Usted debe saber que las cookies pueden recopilar, rastrear y compartir información como su dirección IP, ubicación y otros datos personales con terceros.

#### Nuestro uso de cookies

Utilizamos cookies "técnicas" que permiten ejecutar funciones, opciones y servicios del sitio web y cookies de "análisis" para generar estadísticas sobre las visitas y usos del sitio web.

Quisiéramos utilizar cookies adicionales de:

- Cookies de **"personalización"** para que usted acceda al sitio web utilizando sus configuraciones previas,
- Cookies "publicitarias" para gestionar el uso de espacios publicitarios, y
- Cookies de **"publicidad comportamental"** para elaborar un perfil de su usuario rastreando su navegación en internet.
- "Comprehension salience" (T1): It includes exactly the same information as the previous case, but the information regarding what cookies are and what they do is shown in a box on the right side of the message (Figure 19).

#### Figure 19: "Comprehension salience" design

#### Consentimiento

#### Nuestro uso de cookies

Utilizamos cookies "técnicas" que permiten ejecutar funciones, opciones y servicios del sitio web y cookies de "análisis" para generar estadísticas sobre las visitas y usos del sitio web.

Quisiéramos utilizar cookies adicionales de:

- Cookies de "personalización" para que usted acceda al sitio web utilizando sus configuraciones previas,
- Cookies "publicitarias" para gestionar el uso de espacios publicitarios, y
- Cookies de "publicidad comportamental" para elaborar un perfil de su usuario rastreando su navegación en internet.

#### ¿Qué son las cookies?

Las cookies son archivos de texto que permiten guardar y enviar información desde un navegador. Usted debe saber que las cookies pueden recopilar, rastrear y compartir información como su dirección IP, ubicación y otros datos personales con terceros.

3. "Legal" (T2): Informing about privacy rights could affect the levels of acceptance of cookies. In this way, it includes a message that promotes the

protection of personal data and mentions that the protection of personal data is a fundamental right, indicating that the treatment and protection of personal data must be carried out in the manner and conditions determined by Law (Figure 20).

#### Figure 20: "Legal" design

#### Consentimiento

#### ¡Proteja sus datos personales!

La protección de sus datos personales es un derecho fundamental. Además, el tratamiento y protección de estos datos se debe efectuar en la forma y condiciones que determine la ley.

#### Nuestro uso de cookies

Utilizamos cookies técnicas que permiten ejecutar funciones, opciones y servicios del sitio web, además, cookies de análisis que nos permiten generar estadísticas sobre las visitas y usos del sitio.

Quisiéramos utilizar cookies adicionales de:

- Cookies de **"personalización"** para que usted acceda al sitio web utilizando sus configuraciones previas,
- Cookies "publicitarias" para gestionar el uso de espacios publicitarios, y
- Cookies de "publicidad comportamental" para elaborar un perfil de su usuario rastreando su navegación en internet.
- "Social Norm" (T3): It considers the evidence collected on the impact of social norms of the minority. For this, the message informs that a percentage close to 1% of the people who enter the website reviews the privacy policy (Figure 21).

#### Figure 21: "Social norm" design

#### Consentimiento

¿Sabía Ud. que sólo el 1% de las personas que ingresan a este sitio revisan las políticas de privacidad?

Nuestra política de privacidad informa el procesamiento que se da a los datos personales de las personas e informa sobre el uso de cookies en el sitio.

#### Nuestro uso de cookies

Utilizamos cookies técnicas que permiten ejecutar funciones, opciones y servicios del sitio web, además, cookies de análisis que nos permiten generar estadísticas sobre las visitas y usos del sitio.

Quisiéramos utilizar cookies adicionales de:

- Cookies de **"personalización"** para que usted acceda al sitio web utilizando sus configuraciones previas,
- Cookies "publicitarias" para gestionar el uso de espacios publicitarios, y
- Cookies de "publicidad comportamental" para elaborar un perfil de su usuario rastreando su navegación en internet.