NOVA IMS Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

GDPR in Portugal

Analysis of citizens' perception about privacy

Maria Helena da Silva Alves

Dissertation presented as partial requirement for obtaining the Master's degree in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

GDPR IN PORTUGAL:
ANALYSIS OF CITIZENS' PERCEPTION ABOUT PRIVACY

by

Maria Helena da Silva Alves

Dissertation presented as partial requirement for obtaining the Master's degree in Information Management, with a specialization in Marketing Intelligence.

Advisor: Professor Doutor Flávio Pinheiro
Co-advisor: Professor Doutor Bruno Damásio

July 2021

DEDICATION

Aos meus avós.

Aos meus pais.

À minha irmã.

Ao Luís.

ACKNOWLEDGEMENTS

A realização deste trabalho foi impulsionada por várias pessoas, a quem aproveito para deixar o meu reconhecimento e profundo agradecimento. Peço desde já desculpa pela utilização repetitiva da palavra *agradeço*, mas não encontrei sinónimo à altura.

Agradeço, em particular, aos meus pais por todo o amor e valores que me transmitiram e pelo apoio e dedicação incondicional durante toda a minha vida. Uma caminhada nem sempre justa, mas firme na honestidade e na importância da família. Ensinaram-me a lutar pelos meus sonhos, a ser humana e a aproveitar a viagem. O meu enorme obrigada!

Agradeço à Anita, que além de ser a melhor irmã com que podia sonhar, a minha melhor confidente e companheira, tira os melhores cafés do mundo. O futuro é teu, miúda!

Agradeço ao Luís, por tudo, todos os dias: a paciência, a dedicação, a resiliência, as noites mais longas e o amor. A minha vida é mais bonita por caminhar a teu lado.

Agradeço à minha família toda a partilha e o amor.

Agradeço à Mónica, pelo exemplo de resiliência, de garra e amizade.

Agradeço aos meus amigos de sempre e aos amigos que a Nova IMS me trouxe e com quem partilhei toda esta jornada.

Agradeço à minha equipa na Vision-Box – *Epsílon* –, por todas as aventuras nestes dois anos.

Agradeço aos meus Professores, especialmente aos Professores Flávio e Bruno, pelo apoio e orientação nesta dissertação. À Professora Paula Veiga por me ter incentivado sempre a agarrar novos desafios, em particular este, e à Professora Carla Sá por todo o profissionalismo, empatia e conhecimento. À Professora Benedita Ferreira, ao Professor Carlos Lima, à Professora Maria da Luz, à Professora Manuela Fernandes e à Professora Teresa Lopes, que partiu demasiado cedo. Às minhas treinadoras: Professora Eliana Morais, Professora Sandra Freitas, Professora Elisabete Martinho e Professora Paula Silva. Tive a sorte de ter excelentes professores durante o meu percurso académico, que muito me ensinaram e tiveram um papel essencial no meu crescimento.

Agradeço ainda a todas as pessoas que aceitaram responder aos questionários propostos.

Muito obrigada!

RESUMO

Esta dissertação foi desenvolvida no âmbito da frequência do Mestrado em Gestão de Informação com Especialização em Marketing Intelligence.

O objetivo deste trabalho é analisar a perceção sobre privacidade e o RGPD na população adulta portuguesa e explicar o Paradoxo da Privacidade num caso de estudo sobre a aplicação StayAway Covid. Iniciando com uma Revisão de Literatura dividida em três principais secções: Era da Internet (onde se explora os progressos da Internet até aos dias de hoje), Privacidade dos Dados (do conceito de privacidade à necessidade de regulação) e Regulamento Geral de Proteção de Dados.

Para responder às questões da pesquisa, 2 questionários foram preparados e partilhados através das redes sociais. O primeiro visava perceber a perceção dos participantes sobre privacidade e RGPD (n=271). O segundo procurava explicar o paradoxo da privacidade aplicado à adoção da aplicação de Contact Tracing StayAway Covid por utilizadores das redes sociais (n=115).

Os resultados mostram que há falta de literacia para a privacidade na amostra estudada e foi encontrado um grupo de 'Ativistas da Privacidade' na mesma. Adicionalmente, relativamente ao Paradoxo da Privacidade, podemos concluir que o medo de perder a privacidade pode bloquear a adopção de novas tecnologias.

PALAVRAS-CHAVE

Privacidade de dados; Proteção de dados; RGPD; Paradoxo da Privacidade; Privacidade

ABSTRACT

This dissertation was developed on the scope of the Master's in Information Management with Specialization in Marketing Intelligence.

The main objective of this thesis is to analyze the perception of privacy and GDPR on the Portuguese adult population and explain the Privacy Paradox on a case study about the StayAway Covid app.

The first section contains a Literature Review, divided into 3 thematic: Era of the Internet (where Internet progress is explored), Data Privacy (from the concept of privacy to the need of regulation), and GDPR.

To answer the research questions, 2 questionnaires were prepared and shared through Social Networks. The first one envisions understanding the perception of participants about privacy and GDPR (n=271). The second one tried to explain the Privacy Paradox between social media users (n=115).

The results demonstrated that there is a lack of privacy-related literacy in the sample and a 'Privacy Actives' group was found. Additionally, and regarding the Privacy Paradox, we can conclude that the fear of losing privacy may block new technology adoption.

KEYWORDS

Data Privacy; Data Protection; GDPR; Privacy Paradox; Privacy

INDEX

1. Introduction 1
2. Literature review 3
2.1. Era of Internet 3
2.1.1 The invention of the Internet 3
2.1.2 From the Internet of Computers to the Internet of People 5
2.1.3 Internet of Things and the paradigm of Big Data 7
2.1.4 Evolution of the Internet: are we on the good path? 8
2.1.5 From the ubiquity of the Internet of Things to the need for regulation 8
2.2. Data Privacy 9
2.2.1 The concept of privacy 9
2.2.2 Privacy in the modern world 11
2.2.3 Personal data: what does it mean? 15
2.2.4 Data Protection 15
2.2.5 European regulation 16
2.3. General Data Protection Regulation 17
2.3.1 Objectives of General Data Protection Regulation 17
2.3.2 The rights for the data subjects 18
Transparency and modalities 18
Information and access to personal data 19
Rectification and erasure 21
Right to object and automated individual decision-making 22
2.3.3 New regulation: main changes and challenges 22
2.3.4 Challenges to comply with the new regulation: from theory to practice 23
2.3.5 Organizations 24
2.3.6 Privacy, data protection, and brands' trusting 26
3. Methodology and analysis 27
3.1. Perceived impact for citizens 27
3.1.1. The notions of privacy and GDPR implementation in Portugal 27
Methodology and data collection 29
Data treatment and analysis 30

Participant's profile 31
Usage of Internet 32
Privacy 32
Privacy and smartphones 35
General Data Protection Regulation 36
General Data Protection Regulation and its application 38
Results' Discussion 40
3.1.2. Privacy paradox: the usage of StayAway Covid application 46
Methodology and data collection 49
Data treatment and analysis 51
Participants' profile 51
Measures to control the pandemic in Portugal 53
Use of StayAway Covid 54
StayAway Covid and Privacy 55
Results' Discussion 56
4. Conclusion 61
4.1. Limitations 62
4.2. Recommendations for future work 62
5. References 63
6. Annexes 70
6.1. Questionnaire perceived impact for citizens 70
6.2. Questionnaire StayAway Covid 83

INDEX OF TABLES

Table 1: Evolution of Internet (Mowery & Simcoe, 2002) 4
Table 2: Internet of Computers and Internet of Things (Qin et al., 2016) 7
Table 3: information and access to personal data depending if the personal data is collected or not from the data subject (GDPR, 2016) 20
Table 4: 'The Seven Sins of Personal-Data Processing Systems under GDPR' (Shastri et al., 2019) 24
Table 5: Structure of Questionnaire 'Perceived Impact for Citizens' 29
Table 6: Crosstab Age*SmartphoneSecurer 42
Table 7: Correlation SmartphoneSecurer*Age 42
Table 8: Crosstab LevelOfEducation*SmartphoneSecurer 43
Table 9: Correlation LevelOfEducation*SmartphoneSecurer 43
Table 10: Crosstab OperativeSystem*SmartphoneSecurer 44
Table 11: Correlation SmartphoneSecurer*OperativeSystem 44
Table 12: Correlation PrivacyActive*Age, Level of Education and Smartphone Operative System 45
Table 13: Personal data treated by STAYAWAY SYSTEM (INESCTEC, 2020) 47
Table 14: Structure of Questionnaire 'StayAway Covid' 50
Table 15: Crosstab VoluntaryUse * LossPrivacy 56
Table 16: Correlation between fear of losing privacy and Voluntary usage of Contact Tracing Apps. 57
Table 17: Correlation between Age*LossPrivacy and Age*VoluntaryUse 59
Table 18: Correlation LossPrivacy * Education and VoluntaryUse*Education 60

INDEX OF FIGURES

Figure 1: Age of participants 31
Figure 2: Level of Education of participants 31
Figure 3: Infographics – Privacy and Internet Usage 33
Figure 4: Top 5 companies with the best and the worst behaviors regarding data protection (respondents' opinion) 34
Figure 5: Channels to learn about GDPR 36
Figure 6: Privacy Police on websites 37
Figure 7: GDPR Implementation: security and transparency 38
Figure 8: GDPR and requests to companies 39
Figure 9: Cumulative number of downloads of StayAway Covid app, between the 1st of September 2020 and the 10th of February 2021. (Source: INESC TEC with data from official stores) 48
Figure 10: Age range of survey participants 52
Figure 11: Academic Background of participants 52
Figure 12: Suitability of measures 53
Figure 13: Weight of measures on daily routine 54
Figure 14: Voluntary Usage of App 55
Figure 15: Privacy issues and contact tracing apps 57
Figure 16: LossPrivacy * Age Bar chart 58
Figure 17: LossPrivacy*Education bar chart 60

LIST OF ACRONYMS AND ABBREVIATIONS

API	Application Programming Interface
CCTV	Closed-circuit television
CDO	Chief Data Officer
CNCS	Portuguese National Cybersecurity Centre
CNPD	Portuguese Data Protection Authority
COVID-19	Coronavirus disease (2019)
DCT	Digital contact tracing
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
EU	European Union
GDPR	General Data Protection Regulation
HTML	Hypertext Markup Language
INESC TEC	The Institute for Systems and Computer Engineering, Technology and Science
IoT	Internet of Things
ISPUP	Institute of Public Health of the University of Porto
OECD	Organization for Economic Cooperation and Development
UN	United Nations
US	United States
www	World Wide Web

1. INTRODUCTION

Thomas Cooley wrote, in 1879, that individuals have the 'right to be let alone'. (Cooley, 1879) The recently remarkable technological developments the world undergone implied a significant change in the concept of privacy. According to United Nations (UN), it is estimated that 50% of the world population has access to the Internet, and increasingly more activities are made using it as a medium. Hence, it is important to ensure the online security of individuals' personal information. Even if an individual decides to not use the Internet, he can see his data being shared by third parties through the internet. Indeed, the era of Big Data and the 'Internet of Everything' massified the access to multiple data sources and unprecedented data volumes to work with and extract value, but also brought the need for the development of clear Data Protection and Privacy regulations.

To ensure appropriate data privacy regulation, we are witnessing the worldwide emergence of Global Privacy Laws. In that sense, we can highlight the *General Data Protection Regulation* (GDPR, 2016), the *Canadian Personal Information Protection and Electronic Documents Act* (PIPEDA, 2000) and the *Colorado Data Privacy Act* (2018). Several more Global Privacy Laws are currently under discussion, in countries such as the United States of America, Chile, New Zealand, India, and Brazil. The General Data Protection Regulation was officially implemented within the European Union on the 25th of May of 2018.

Throughout the 28 members of the European Union, and covering all the business sectors, the *General Data Protection Regulation* (GDPR) is the law that certifies that citizens have the right to data protection during the Digital Era, following article 16(1) of the Treaty On The Functioning Of The European Union, where it is mentioned that '*Everyone has the right to the protection of personal data concerning them*' (European Union, 2012). The main objective of GDPR is to give more control to people of their personal data and to increase the confidence in the process of using personal data by firms.

The application of the law has brought significant changes in the internal processes and methodologies inside the companies. In a world that changes at a hallucinate rhythm, companies are facing several challenges to comply with this law.

At the same time, customers have observed different changes happening, being part of some: consent e-mails for unlocking access to web services; the requirement for users to accept cookies; or the right to be forgotten.

Companies are facing an extra challenge: allied to the changes needed to comply with European Regulation, people are more aware of the risks and attentive to what companies do with their data. Brands – such as *Apple* – are trying to position themselves as a data protectionary company while raising awareness about the current non-existence of privacy. This important trend – being Privacy considered a Fundamental Right - will bring important discussions in the future.

This dissertation aims to understand how citizens perceive the changes brought up by GDPR, what is the knowledge acquired about privacy, and how can GDPR block future adoption and digital transformation. Considering that citizens are consumers, and their perception and behaviors may impact businesses, it is important to understand how this thematic affects their understanding of the topic.

Within this work, two different studies were performed: the first one aims to understand the perception and knowledge of citizens about GDPR and the second one intends to understand the usage of the StayAway Covid application.

2. LITERATURE REVIEW

2.1. Era of Internet

The way the world behaves was significantly impacted by technological evolution.
At the beginning of the 20th Century, the use of computers was proliferated with war objectives. From the time of Mark I, the first known multipurpose computer and today, the world assisted to a notable technologic revolution. This revolution had a broad effect, and it was the basis of considerable changes in different sectors, for example in society, culture, education, business, healthcare, transportations, and communications. Nowadays, it is unimaginable to project the world without technology. From the smallest activity of the day to the device used to monitor our heartbeat in real-time, our daily life is dependent on technology. This phenomenon was reinforced through the evolution of the electronic sector, informatics, and telecommunications (Roza, 2018).
The advent of telecommunications, with strong growth after 1980, with the digitalization, had a significant impact, allowing users to communicate through voice, images, and data (Roza, 2018). When going back to the beginning of the millennium, there were not smartphones, connected devices, or e-commerce (except Amazon, which was created in 1994). Analyzing the exponential evolution is worldwide accepted that there is a common factor: the invention of the Internet.

2.1.1 The invention of the Internet

After the invention of the modern computer, the Department of Defense of the United States started to support research to find and develop a technology with the capability of supporting the limited computing resources used in their center. The strong collaboration between researchers from academic, defense, and industrial sectors, the size of the domestic market, and the robust computer hardware and software industries were catalysts of the development of the Internet (Mowery & Simcoe, 2002).

Period	Context	Critical developments
1960 – 1985	▪ Mainly used by computer scientists and engineers. ▪ Focus on developing and deploying.	▪ Development of digital packet switch (called IMP). ▪ Release of e-mail by ARPANET. ▪ Deployment of CYCLADES.
1985 - 1995	▪ Started to be used by researchers. ▪ Focus on developing and expanding the core infrastructure.	▪ Moved from public management to private management. ▪ Introduction of The National Science Foundation Network (NSFNET). ▪ The advent of private access market, using the telecommunications infrastructure.
1995 - 2002	▪ Public use.	▪ Privatization of NSFNET. ▪ Initial stock offer of Netscape. ▪ Diffusion of World Wide Web (WWW). ▪ The emergence of commercial content. ▪ Development of applications.

Table 1: Evolution of Internet (Mowery & Simcoe, 2002)

The chronological milestones on the evolution of the Internet presented (Table 1), is divided into three phases, according to Mowery & Simcoe (2002): the first one comprehends the period between 1960 and 1985, the second one between 1985 and 1995, and the last one between 1995 and 2002 (the date of the publication of the article). In the early 1960s, a digital packet switching (the first one was called Interface Message Processor (IMP)) was developed and brought benefits in performance and consistency when compared with analog networks. In 1972, ARPANET launched electronic mail (e-mail).

The Internet, originated to be used by the US during the Cold War, was linked with military computer installations in the US and connected to universities involved in their research. Finding that the Internet was an excellent channel to exchange information, academics were the main users between the end of the 70s until 90s (Leiner et al., 2009).

Between 1985 and 1995, with the increase of the users and applications, other challenges arose, and it was needed to change the approach: from improving and implementing the network to developing and expanding the infrastructure to answer the rising demand by academics and the military.

The creation of the National Science Foundation's national Internet backbone (NSFNET) in 1986, a roughly organized community of networks whose goal was to support the sharing of national scientific computing resources, data, and information (Mills, 1987), and the advent of private access market that used the telecommunications infrastructure were the main changes during these years (Mowery & Simcoe, 2002).

According to Mowery & Simcoe (2002), the third phase of the evolution of the Internet began in 1995 and this period started with the privatization of NSFNET and the initial stock offer of Netscape. Within this period, the fast diffusion of the Web potentiated the development of applications and business-related content.

The proliferation of the use of the Internet worldwide was possible after the US military find new ways of communicating: Tim Berners-Lee realized that the exchange of multimedia would be a great contribution to what the Internet allowed to do and built the World Wide Web, through the first version of HTML (Leiner et al., 2009).

The spread of the World Wide Web brought the opportunity to solve several problems faced by society. The production of information became horizontal, decentralized, and interactive instead of being hierarchical (Dias, 2005).

Internet and the Web completely changed the way the world works nowadays.

2.1.2 From the Internet of Computers to the Internet of People

The first years after the Internet's invention were marked by significant improvements in computer hardware, software, and networking technologies. These upgrades were responsible to make computing technologies accessible to the market at low prices (Mowery & Simcoe, 2002).

This period was strongly impacted by technological evolution, mainly focused on computers. After the ARPANET project, which envisioned to develop practices on interconnecting computers, sharing research, and link computers, there were significant efforts made to build the Internet that we have nowadays, is a global system of networks

that interconnect computers (Ibarra-Esquer, González-Navarro, Flores-Rios, Burtseva, & Astorga-Vargas, 2017).

Based on these developments, a new opportunity arose and, in 1999, Kevin Ashton made a presentation called 'Internet of Things', to explain the link between the use of RFID in Procter & Gamble's supply chain and the Internet. According to the authors, (Ibarra-Esquer et al., 2017), Ashton presented a vision where, using specific technologies like sensors or RFID, computers would observe, identify and understand how the world works, through data collected and transformed into information.

In 2005, the International Telecommunication Union (ITU) published the *Internet of Things* report. This report helped to prospect technological advances that would facilitate the promise of a connected world, with 'always on' communications and devices capable to provide personalized information to consumers, worldwide (ITU, 2005).

Kevin Ashton, the first person known to mention the term *Internet of Things*, clarified his idea about it: '(…) Today computers—and, therefore, the Internet—are almost wholly dependent on human beings for information. Nearly all the roughly 50 petabytes (a petabyte is 1,024 terabytes) of data available on the Internet were first captured and created by human beings—by typing, pressing a record button, taking a digital picture, or scanning a bar code. Conventional diagrams of the Internet include servers and routers and so on, but they leave out the most numerous and important routers of all: people'. (Asthon, 2010) The author continues arguing that the limited time, attention, and accuracy that people have constitutes an issue to the gathering of data, being important to empower computers to this.

The development of those perspectives was fast and mainly based on three steps (embedded intelligence, connectivity, and interaction). Starting with embedded intelligence: things became able to do actions automatically, for instance, the RFID reader that can get the information recorded on the RFID tag implanted in food. Once embedded intelligence was implemented from a local point of view, the following step was to connect the things, transforming them into smart things. After being able to connect things, the focus was to allow the communication between themselves: they

shall be able to interact and exchange information. This way, the way of communication changed from human-human to human-thing to thing-thing (Tan, 2010).

According to Atzori, Iera, & Morabito (2014), there are three stages of the evolution of IoT, being the mentioned smart objects the beginning of the process of evolution of communication devices. In their article, the authors presented the idea that in the first phase, objects were capable to inform humans about their state, then they interact with an application layer and in the third stage, objects are moving from smartness to a status where they have a social consciousness and acts in a social community of objects and devices.

The vision of Atzori, Iera, & Morabito (2014) converge with the vision of smart integration: deploy solutions that can make people's life easier, working with seamless technology that considers people's context, learn from it, and assume proactive steps according to the situation to prevent human intervention. (Miranda et al., 2015).

Table 2 represents the differences between the Internet of Computers and the Internet of Things in the vision of Qin et al. (2016).

	Internet of Computers	Internet of things
Web & Web of data	▪ People generate	▪ Things generate
Information	▪ People gain	▪ Things gain
Knowledge	▪ People discover	▪ Things discover
Solutions	▪ People propose	▪ Things propose

Table 2: Internet of Computers and Internet of Things (Qin et al., 2016)

2.1.3 Internet of Things and the paradigm of Big Data

'Internet of Things (IoT) will comprise billions of devices that can sense, communicate, compute and potentially actuate. Data streams coming from these devices will challenge the traditional approaches to data management and contribute to the emerging paradigm of big data.' (Zaslavsky, Perera, & Georgakopoulos, 2013)

Nowadays, and especially with the emergence of the Internet of Things, there are billions of devices connected to the Internet that collect and exchange data. (European Commission, 2019)

According to International Data Corporation, in 2025, it may exist 41.6 billion IoT-connected devices, that will generate 79,4 zettabytes of data (a compound annual growth rate of 28,7% during the period 2018-2025). They expect that the main source of data is video surveillance applications, but categories as industrial and medical are gradually generating more data. (International Data Corporation, 2019)

The data collected nowadays benefit from three new characteristics: volume, velocity, and variety. The amount of data generated is increasing and enterprises can manage data sets with petabytes of data, composed not only with Internet data but from other sources, offering a significant variety of entries. For many companies, more important than the volume is the velocity that applications are being able to generate data: real-time or nearly real-time data facilitates rapid insights that are, in some cases, the opportunity to surpass a competitor. (Mcafee & Brynjolfsson, 2012)

2.1.4 Evolution of the Internet: are we on the good path?

The uniqueness of the Internet, with its ubiquity, global reach, the density of information, and universal standards, is not – by itself – capable to be good or bad (Laudon & Traver, 2014). What defines the potential benefits or dangers of the Internet is the way people use it.

As we can find in the work of Drucker (1999), the evolution of technology is really fast, but there are always three particular characteristics present on the Internet with significant impact:

- The ubiquity of data;
- No time frame between the moment a text is produced and published;
- Real-time collaboration.

These facets open the window of multiple challenges that will be developed in the next chapters.

2.1.5 From the ubiquity of the Internet of Things to the need for regulation

One of the most mentioned characteristics of the Internet is ubiquity. Even though the term comes from the Latin root ‘ubique’, which means everywhere, there are different applications around the world. In Europe, ubiquity tends to be understood as ‘available

from all parts of the globe'. On the other hand, in Japan and the Republic of Korea, it represents a universally available communication service. In Japan, for instance, it is accepted that a 'Ubiquitous network society' is 'available anywhere, anytime, by anything and anyone' (ITU, 2005).

Back in 1991, Marc Weiser called 'Ubiquitous Computing' to describe a world where everyday objects would have computer devices integrated, computer usage would be easier (taking advantage of intuitive interfaces), and networks would connect devices. This expression, ubiquitous computing, would be the base to build an era where things would interrelate themselves dynamically.

With the progress in technology, a new vision for machines arose: The Internet of Things (IoT). IoT promised to be the digital revolution of the century: as in the 19th century they learned to do, in the 20th they learned to think, the goal is to assure that in the 21st century they perceive (through metadata) (Sundmaeker, Guillemin, Friess, & Woelfflé, 2010).

The Internet and consequently the information that is gathered have changed the method of communication worldwide. Nowadays, people are online for a significant part of the day. IoT desires to link ubiquitous components, tanging them into people's routines. The opportunity to increase productivity and efficiency (and win money with these developments) and the convenience that it can bring to us is attractive (Williams, Nurse, & Creese, 2016).

However, this continuous collection of information can bring us privacy issues.

These mentioned privacy issues are related to the control of data and worldwide nations are trying to reduce this cyber risk through regulation.

2.2. Data Privacy

2.2.1 The concept of privacy

Privacy, related to private, derives from the word *prīvātus* that means withdrawn from the public life ("Merriam-Webster," 2020).

Privacy has been discussed since primordial times. Analyzing philosophical publications, we can find the privacy concept enlightened in the books about the politics of Aristotle or in the Public and Private distinction provided by John Locke. (DeCew, 2016)

In 1890, the Harvard Law Review (a student-running journal focused on legal issues), published an interesting article about privacy: *'Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone.' Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.''* (Warren & Brandeis, 1890)

In fact, judge Thomas Cooley has recognized that individuals have the 'right to be let alone', on his book 'A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract', in 1879. (Cooley, 1879)

On the 10th of December of 1948, in Paris, the Universal Declaration of Human Rights was stated by the United Nations General Assembly. This declaration, written by worldwide specialists, aimed to define achievements for all peoples and all nations (UN, n.d.). The article 12th of this document defines that 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.' (UN, 1948)

In 1960, William Prosser published a law review article where he presents his definition for privacy, based on the right to be let alone, and divided into four points: 'intrusion upon a persons' seclusion, solitude, or private affairs; public disclosure of embarrassing facts; publicity that places a person in a false light; appropriation of a person's name or likeness for the advantage of another' (Prosser, 1960).

Within the years, numerous concepts for privacy were developed. In 1967, Westin described privacy as the right, for individuals and groups, to define when, how and to what extent of information about themselves can be shared with others (Westin, 1968)

Over the years, it is being hard to define privacy and it seems that it used as a hypernym to related concepts. (Mag, 2011)

Solove, in 2002, argued that the fact that people feel that some aspects of life are private, and we relate these aspects with privacy. However, is this sense of privacy and these aspects of privacy, absolutely private? Considering the importance of the issue not only for policy and legal decisions but for freedom, democracy, individual well-being (…), have developed a conceptualized model to define privacy, collecting and criticizing the existing theories about the issue and defining is own concept of privacy, based on six aspects: 'the right to be left alone; restricted access to one's person (physical person) or possibility to protect oneself from unauthorized access; right to hide certain things from others; control over personal information; protection of one's dignity, individuality and persona; and intimacy – the right to control and limit access to information that concerns intimate relationships and aspects of life.' (Solove, 2002).

2.2.2 Privacy in the modern world

The traditional understanding of privacy, with descriptions and conceptualizations developed before the advent of the Internet, is not prepared to deal with the impactful challenges that arise with technology (Austin, 2002).

The rise of new technologies and their application, allowed with the accessibility to the Internet, made the concept of privacy evolves, and the need for control was aggregated. According to the authors, if a consumer on a digital platform loses control of his personal data, he can say that his privacy was desecrated. (O'Brien & Torres, 2012).

In the last years, we have observed an entirely change in how the world works: the internet and its related developments allowed the business to move to the Internet and making, per example, e-commerce and social media parts of the businesses with high importance.

The supply to consumers is broad: cloud services, smart devices, applications, social media are part of our daily lives.

According to Murumaa-mengel, Pruulmann-vengerfeld, & Laas-Mikko (2014), it is important to pay attention to technology in our daily life, especially to their potentially extensive usage opportunities (how information is used, per example), the eagerness to

be always available to use (mobility and connections), significant number of users and the transformation on the social life, like rituals and routines. The life on the Internet works as an extension of our physical life and people do not realize it, potentializing the dangers for their privacy that may not be noticed. (Murumaa-mengel, Pruulmann-vengerfeld, & Laas-Mikko, 2014)

There are many ways to collect data from the usage of the Internet. One of the most famous is through online social networks. Online social networks are web-based services where users create their own profile and build a list of users with whom they want to share the connection, typically called networks (D. M. Boyd & Ellison, 2007).

Facebook is the leader of online social networks with approximately 2.4 billion active users per month, followed by Instagram with 1 billion monthly, WhatsApp and Facebook Messenger ("www.statista.com," 2020). The experience and connections can vary, from friends (Facebook), followers (Twitter, Instagram), professional (LinkedIn), dating (Tinder) and subscriber (YouTube).

There are three main categories of data, online social networks can collect from users: the profile, connections, and comments. However, and depending on the social network being used, there are other types of information collected: messages, multimedia, hashtags (used as keywords), preferences, feelings, behaviors, groups and location. (D. M. Boyd & Ellison, 2007)(D. Boyd, 2007).

The growth of online social networks caused a complete rethink on boundaries between private and public. Before the Internet, the public scope was related to places: coffees, streets, malls, parks, etc. Nowadays, something public is not necessarily a place, but can be shared to the public in front of computers or through mobile applications. According to Boyd, in 2007, this redefined concept brought significant properties to the context: a) Persistence: what is published today will be online in the future, even if the user changed his ideas or behaviors; b) Searchability: it is easy to find published information on Internet; c) Replicability: information can be copied and transferred to another context; d) invisible audiences: we are not able to control who is observing our online activity (D. Boyd, 2007).

The advent of smart gadgets used as part of the consumers, brought this risk to another level: the highest amount of data collected and a lack of association to privacy risks. According to the authors of a study developed in 2014, in terms of privacy, using a mobile environment is more dangerous than the classic systems (Aditya, Bhattacharjee, Druschel, Erdélyi, & Lentz, 2014).

To understand if mobile applications access to more information than needed, a list of apps and their permissions was analyzed and concluded that users were facing privacy abuses on the sensitive data shared. (Furini, Mirri, Montangero, & Prandi, 2020)

This online focus is not restricted to consumers. Businesses have suffered a complete change in the processes to be online and new sectors born, like sharing economies. Despite the expected changes in the organizations, companies lived a digital transformation to adapt themselves to the market and take advantage on the new possibilities available: new ways to communicate and better models to adapt the communication using data. Nowadays, there is a large range of features that use large information flows to predict decisions (Armando et al., 2019). Advertisers, per example, are using online data about consumers to personalize and target advertisements. Using online data about consumers (websites visited, articles read, videos watched…), advertisers are increasing the quality of the personalization and targeting to sell their products. (Boerman, Kruikemeier, & Zuiderveen Borgesius, 2017)

According to Euromonitor International Top 10 Global Consumer Trends 2020, one of the big trends to the year is related to Private Personalization: consumers are expecting that brands adapt products and services to them, but companies need their personal information to ensure that. Because of that, companies are creating algorithms and improving data collection methods to improve their marketing capabilities. Allied to this, new challenges appear: companies must be transparent with consumers about data collection and its use and consumers seem to be more concerned about privacy issues (Westbrook & Angus, 2020).

Despite the growing fears about privacy and online susceptibility to privacy issues on the theorical community, consumers of online platforms continue to share their

personal information and do not seem to be worried about the possible loss of control. (Rosenblum, 2007)

As reported by Euromonitor International's Lifestyles Survey 2019, between 40-50% of consumers agree that targeted ads based on the online paths are an invasion of privacy. Nevertheless, youngers consider that receive personalized marketing overlaps the risk and are available to share their data to facilitate the process. (Westbrook & Angus, 2020)

This apparently inconsistency between people claiming for privacy's importance and sharing personal data with third parties is called 'Privacy Paradox' (Susan B. Barnes, 2006)

According to Hargittai & Marwick (2016) research, this paradox can be explained by the missing knowledge about the risks, privacy-protective behaviors or the benefits of online self-disclosure, and it is frequently summarized as 'Young people don't care about privacy'. Deeper research on the generational aspect of the paradox, conclude that concerning mobile app environments, the level of engagement for privacy-protective behaviors is similar between youngers and adults and is higher on social media, arguing that generational behaviors cannot justify the existence of the privacy paradox (Madden, M., Lenhart, A., Cortesi, S., & Gasser, 2013)

The *privacy calculus*, the rational balance between pros and cons of disclosing personal data to a company, is in theory affected by market offerings, reduced prices, search costs and perceived harm. Additionally, non-rational factors may influence these decisions. These attitudes may vary on behavioral changes. The authors found that protectionists, per example, give fake data to protect their privacy. Capitalists, in the other hand, shared confusing data to not be invaded by junk e-mails, once they did not find the added value of disclosure real data for them. (Plangger & Montecchi, 2020)

2.2.3 Personal data: what does it mean?

According to the GDPR, personal data means: *'any information relating to an identified or identifiable natural person ('data subject'[1]); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'* (GDPR, 2016).

Analyzing the Working Party 29, it is important to define two elements:

a) Information: the scope of information is broad having in mind that nowadays almost everything can contain information. The operational idea is that information is the sum of data and meaning (Floridi, 2005).

b) An identified or identifiable natural person: this part of the definition extends the definition to data that is not already identified but contains facets that can allow identification.

According to Benfenatki, Goncalves, Nicolas, Winckler, and Bernard, personal data can be financial, administrative, related to identity (name, date of birth, card citizen number), biometric elements, connection data, localization, activity data among others and can be described as explicit, collected or generated, according to the root source. (Benfenatki et al., 2018)

2.2.4 Data Protection

It is globally known that companies are using data to develop their businesses and, in many cases, increase the effectiveness of their work.

In August 2019, the biggest social network Facebook, removed the slogan that was always present in its home page 'It's free and will always be' to 'It's quick and easy'. The terms and conditions of the platform are more specific about the thematic: '*We don't charge you to use Facebook, or the other products and services covered by these Terms.*

[1] According to the GDPR, data subject is any identified or identifiable natural person, covered by GDPR.

Instead, businesses and organizations pay us to show you ads for their products and services (…) We use your personal data to help determine which ads to show you.' ("Facebook: Terms and Conditions," 2020). Facebook is using our personal data to target ads that companies want to show us.

It is commonly accepted that personal data is being collected, stored and managed. Data protection regulations help to define the standards to treat it, to ensure that data is secure, safe and accurate.

Even though the entities that are owners of citizens' personal data should protect personal data, citizens shall think about it before publishing and share it.

2.2.5 European regulation

The need of regulation to personal data is not recent. With the evolution of technology, the importance given to personal data has been growing.

After the Second World War, to protect the three main (and common) principles of the state members (pluralist democracy, respect to the Human Rights and open economy), the Organization for Economic Cooperation and Development (OECD) have created the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. These guidelines, published in 1980, were designed to help the adaptation to technological changes, perceived at the time. They tried to define the standards to collect and manage personal data. (OECD, 1980)

In 1995, the European Union developed a more recent and adapted regulation to be applied to all the state members, through the Data Protection Directive 95/46/EC (DPD) (European Union, 2016). This Directive aimed to protect the citizens of all the state members, regulating the process of collection of personal data (Ryz & Grest, 2016). Additionally, this law was designed to ensure the rights and freedom of citizens related to the data treatment, assuring the free circulation of personal data between the member states (European Union, 2016).

Despite the added value brought by DPD, with the globalization and technological evolution, the processes related to personal data have been developed and a new regulation was settled to ensure a higher level of protection – The General Data Protection Regulation.

2.3. General Data Protection Regulation

The General Data Protection Regulation is a Privacy Law applied within all European Union in 2018, aiming to replace the Data Protection Directive. This law defines the requirements for the processes of collecting, store, and manage personal data.

This law applies to European companies and organizations, and to companies and organizations of other regions that process personal data of European citizens.

Within GDPR, some rights were added to assure cybersecurity to EU citizens, which will be discussed within this chapter.

This new Regulation obliged companies to change their departments and reorganize the way they manage data. After a challenging path to be compliant on time, it is important to understand the perceived impact of those changes.

One conclusion seems to be accepted 'European-Union-wide': with the increasing of the value of personal data to the market, this regulation defines the lifecycle of data to protect the privacy of the citizens.

2.3.1 Objectives of General Data Protection Regulation

The article 8 (1) of the Charter of Fundamental Rights of the EU and the 16(1) of the Treaty on the Functioning of the EU defined that each person has the right of protection regarding the treating of him or her personal data (GDPR, 2016).

'Article 1 – Subject-matter and objectives

1. *This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.*
2. *This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.*
3. *The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.'*
   (GDPR, 2016)

GDPR was built to contribute to the development of an area of freedom, security, justice and economic union where the social and economic progress, the consolidation and convergence of internal markets and the well-being of populations are appreciated (GDPR, 2016).

This regulation was developed to ensure the protection of personal data but reserving the needed respect to the other rights and freedoms (and respecting the principle of proportionality). (GDPR, 2016)

With the rapid technological developments, globalization and socioeconomic integration within the European state members, the flows of personal data transferred beyond borders have increased and new challenges on data protection arise, since the amount of data collected and its sharing. This regulation helps to ensure that personal data can circulate freely with high level security. (GDPR, 2016)

To respond to the new challenges, it was agreed that the processes shall be equivalent between Member States (this was not verified with the Directive 95/46/EC, once we observed several local guidelines). This centered regulation helps to offer legal guidelines with transparency, giving confidence to the market, ensuring the same rights and obligations to the citizens and useful collaboration with the supervisory authorities (GDPR, 2016).

2.3.2 The rights for the data subjects

Transparency and modalities

The article 12 'Transparent information, communication and modalities for the exercise of the rights of the data subject' defines that the communications provided shall be concise, transparent, intelligible, and easily accessed. The language shall be clear and plain, especially if the data subject is a child. The controller shall facilitate the processes available to ensure the data subjects' rights, that englobes, per example, ways of request and obtain freely access, rectification, or erasure of personal data. This process shall be available to do electronically (GDPR, 2016).

Information and access to personal data

The articles 13 and 14 of GDPR aim to clarify the modalities of information and access to personal data. These articles make a clear difference depending on the source of the information, having the personal data being gathered from the data subject (article 13) or not (article 14). (GDPR, 2016)

These differences are mentioned on the table 3:

	Personal data collected from the data subject	Personal data not collected from the data subject
The identity and the contact details of the controller	When personal data is obtained	All the time
The contact details of the data protection officer	When personal data is obtained	All the time
The purpose of the processing	When personal data is obtained	All the time
The categories of personal data concerned		All the time
The recipients or categories of recipients of the personal data	When personal data is obtained	All the time
The intention of transferring personal data to a recipient in a third country or international organization	When personal data is obtained	All the time
When the process is justified by legitimate interests, if they are chased by the controller or by a third party	When personal data is obtained	All the time
The period of storage	When personal data is obtained	All the time
The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability	When personal data is obtained	All the time

	Personal data collected from the data subject	Personal data not collected from the data subject
The right to withdraw consent at any time	When personal data is obtained	All the time
The right to complain with the supervisory authority	When personal data is obtained	All the time
If the gathering of personal data is a contractual requirement and if the data subject is obliged to provide personal data and the consequences of the processing	When personal data is obtained	
Existence of profiling	When personal data is obtained	All the time
Source of personal data		All the time
Further processing for a different purpose	Before the processing	Before the processing

Table 3: information and access to personal data depending if the personal data is collected or not from the data subject (GDPR, 2016)

Despite the mentioned differences regarding the source of personal data, the data subject has the right, all the time, to access to the personal data stored and to be informed regarding:

'Article 15, 1º

a. *the purposes of the processing;*
b. *the categories of personal data concerned;*
c. *the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;*
d. *where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*

e. *the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;*

f. *the right to lodge a complaint with a supervisory authority;*

g. *where the personal data are not collected from the data subject, any available information as to their source;*

h. *the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.' (GDPR, 2016)*

Additionally, the data owner and its controller shall, when requested, deliver a copy of personal data for free. (Mannhardt, Petersen, & Oliveira, 2018)

Rectification and erasure

When the personal data concerning the data subject is not correct or it is not complete, he or she has the right to edit it and or complete it. (GDPR, 2016)

In addition, and under some conditions, the data subject has the right to erasure ('right to be forgotten'). As the article 17 clarifies, the controller has the obligation to delete permanently personal data when: '

a. *the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;*

b. *the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;*

c. *the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);*

d. *the personal data have been unlawfully processed;*

e. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

f. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).' (GDPR, 2016)

Additionally, the data subject has the right to ask for restrictions on processing under the points described in article 18 and the right to data portability, described by the right of receiving the personal data provided to a controller and share it with another controller. (GDPR, 2016)

Right to object and automated individual decision-making

According to GDPR (2016), each citizen has the right to object to the processing of their own personal data, at any time. The exception for this right is mentioned in article 21 (6), which explains that the data subject has the right to object except if that specific processing is essential for reasons of public interest.

Moreover, article 22 refers that the data subject has the right to not be part of decision-making based on automatized processes, including profiling unless i) is needed to ensure a contract between the data subject and the data controller; ii) is authorized by European Union or State; c) is based on previous explicit consent. (GDPR, 2016)

2.3.3 New regulation: main changes and challenges

One of the main changes is that, instead of the Directive 95/46/CE, this regulation is applied besides all the companies established in the EU, to the companies located outside of the EU that provide any service or good or monitor to its citizens. GDPR shall be applied to every organization that treats personal data. With these changes, some companies like Instapaper, Klout, and Unroll.me finished their activity in Europe. (Shastri, Wasserman, & Chidambaram, 2019)

GDPR brought many rights to data subjects: a) Right to be informed, b) Right to Access, c) Right to Rectification, d) Right to Erasure, e) Right to Restriction of Processing, f) Right to Data Portability, g) Right to Object, h) Automated Individual Decision Making, i) Right to Withdraw Consent. (GDPR, 2016)

To be compliant with all the changes, companies faced many organizational changes that will be analyzed during the development of this work.

2.3.4 Challenges to comply with the new regulation: from theory to practice

Shastri, Wasserman & Chidambaram (2019) wrote an article called 'The Seven Sins of Personal-Data Processing Systems under GDPR', where they explain the behavioral changes that companies find between the theory and the practice of GDPR application. The main conclusions can the analyzed in Table 4: 'The Seven Sins of Personal-Data Processing Systems under GDPR' (Shastri et al., 2019).

Practice	Motivation for the practice	Articles that limit the practice under GDPR	Practical effect
Data storage	With the evolution of analytics (machine learning and big data), data started to be more valuable in the market.	▪ 5(1)(E) ▪ 13 ▪ 17	Personal data shall have a time of expiration and data subjects can require its deletion when they want.
Reuse data	Companies design processes where they collect data once and they can use it indiscriminately transversely with different systems	▪ 5(1)(B) ▪ 6 ▪ 21	Each personal data collected shall have its purpose clearly defined all the time.
Sharing data	With the increase of the value of data to business, its sharing makes money.	▪ 20 ▪ 14	When an organization uses data that was not collected by them, data subjects have the right to access this information and ask for its portability.
Changes on data processing models	In a sector that moves fast, not all companies were careful about data processing	▪ 35 ▪ 36	When an organization wants to use new technologies or change the existing systems, but they process personal data, they shall evaluate

Practice	Motivation for the practice	Articles that limit the practice under GDPR	Practical effect
			the risks to ensure the compliance of processing.
Hiding data breaches	Facing an issue with privacy or a data breach, companies usually hide them from the data subjects.	▪ 5 ▪ 33 ▪ 34	Organizations have to create measures to ensure the security of their systems and they shall notify their breaches in 72 hours.
Algorithmic decision-making	With the technological evolution, algorithmic decision-making brought unquestionable benefits to businesses and to society.	▪ 15 ▪ 22	Data subjects have the right to ask for explanations about the logic involved and its consequences.

Table 4: 'The Seven Sins of Personal-Data Processing Systems under GDPR' (Shastri et al., 2019)

2.3.5 Organizations

Companies had time to prepare for GDPR's implementation. In the beginning, companies had to identify where and why they use personal data and if they can manage it. After ensuring that part, organizations started to define processes where they comply with the regulation. The expectation was that they would develop high-level governance measures, as privacy impact assessments, to ensure the required obligations and protect customer's data. (Beckett, 2018)

Companies were encouraged to improve their document management processes, save all personal data entries, and create their own conduct codes. Additionally, GDPR implementation was a huge opportunity to reduce costs (on data storage, per example), improve the quality of analytical knowledge, increase the confidence of clients (being compliant means the data is being carefully saved), among others. (Beckett, 2018)

The introduction of the Data Protection Officer by the GDPR constitutes a change for organizations. Even not being required by all the companies, this person shall be independent and with a significant level of knowledge and expertise. (UTAIL / JurisAPP, 2019)

According to the report developed by UTAIL/ JurisApp (2019) 'Avaliação do Impacto Legislativo – Regulamento Geral de Proteção de Dados', the implementation of GDPR required an additional effort to the organizations, mostly with:

- Implementation costs (diagnosis/requirements collecting, data treatment recordings, revision of privacy information and contracts, revision of procedures to ensure data subjects' rights, implementation of procedures to answer to the requests of data subjects, process of consent, data security, elaboration of the code of conduct and its certification and preparation for internal auditing)
- Introduction of the role Data Protection Officer
- Notification of data breaches
- Education

According to a report developed by the Multistakeholder Expert Group (EU) (2019), most organizations reveal they made considerable investments to be compliant with GDPR. Especially for small and medium-sized enterprises (SMEs), they had significant costs to adapt to the new regulation, and many of them mentioned they had to contract services from external consultants to understand the differences and apply them (revealing a lack of human and economic resources to be compliant). According to the same report, it is still hard to predict the impact of GDPR on oncoming innovations, but the risk of incurring heavy sanctions may affect innovation negatively. (Multistakeholder Expert Group (EU), 2019)

Especially on the health field, with its strong influence on ethics, was needed to work on the processes to implement pseudonymization (already in use in some projects), anonymization, and consent, requiring an investment of resources to assure people keep their trust in the medical research community and in the integrity of their personal data. (Carter, Laurie, & Dixon-woods, 2015; Mark, Rumbold, & Chb, 2017)

An empirical study developed to analyze the impact of GDPR on websites, by comparing the 500 most visited ones in each of the 28 countries that are part of the EU, concluded that there generally, it has a positive effect on the transparency of websites (+4.9% of websites implemented privacy policies and/or started informing their visitors about cookie's practices). However, the same study concluded that the privacy policies were

updated in May 2018 in 50% of and in 60% of the websites there was not any change during 2016 and 2017 (the GDPR's two-year grace period). Despite the numbers presented, the authors realized that the practices seem to be similar: the tracking level is analogous and most of the websites use opt-out consent mechanisms. For web consumers in the EU, the main difference is an increase in cookie consent notifications and the different features they offer. (Degeling et al., 2019)

2.3.6 Privacy, data protection, and brands' trusting

With technology developed, companies can collect more and different data from their customers. At the same time, methodologies were improved to monetize this data.

With GDPR implementation, consumers may recover the feeling of controlling their data.

A Consumer Privacy Study, conducted by Cisco in 2019, found a new actor related to the topic: Privacy Active. A person that admits being concerned about privacy, is eager to act to ensure it and can leave a company due to their behavior related to data (Cisco Secure, 2020). The same study refers there is a generational impact on the profile of Privacy Actives. Population under 40 years old, looking for a customer experience where privacy takes an important impact and the way data is treated represents a valuable metric on how they see the company. (Cisco Secure, 2020)

Being an important group of consumers, 29% on the sample analyzed for the mentioned report, companies shall start considering them. (Cisco Secure, 2020)

The negative effects of privacy concerns raised by consumers and consequent lack of trust can be resumed in loss of revenue, risk of litigation, and data foreclosure. (Bleier, Goldfarb, & Tucker, 2020)

3. METHODOLOGY AND ANALYSIS

Despite other countries' efforts to regulate data protection, GDPR is the first broad regulation applied in a union of different states.

Due to the extension and exigence of norms imposed, organizations that manage data had the challenge to prepare all the changes to comply with the regulation.

At the same time, the perceived impact of the regulation for citizens is not clear.

3.1. Perceived impact for citizens

The main objectives of this analysis are to understand:

i. The importance of privacy and data protection
ii. The perceived effects on data protection and privacy after GDPR application
iii. If citizens understand what GDPR brings
iv. If the Privacy Paradox is verified with the GDPR through two main approaches:
    - The valuation between privacy and customized online services
    - The valuation between privacy/data protection and public health (analyzing the use case of the app of contacts tracing for COVID-19)

Descriptive research will be used to measure the perceived impact for citizens, particularly through quantitative research. Quantitative research is used to gather data that will be processed through statistical techniques (Bhat, 2019).

The data was collected through a survey that will be distributed online to a random sample. The objective number of answers is 275. The detailed results are presented on 3.1.1: The notions of privacy and GDPR implementation in Portugal. To test the Privacy Paradox, detailed in 463.1.2: Privacy paradox: the usage of StayAway Covid application a survey shared through social media aims to collect answers from different respondents.

3.1.1. The notions of privacy and GDPR implementation in Portugal

The GDPR implementation raised a significant level of discussion on how European Citizens and Companies deal with privacy and data protection.

Despite the strength of being a regulation, it is important to evaluate if there are significant improvements in the citizens' perception and behaviors after its implementation.

This section aims to answer the following Hypothesis:

Research Question 1: Individuals have literacy on online privacy issues

With the globalization and democratization of the Internet, the access to the Internet, and the amount of data collected, literacy for privacy issues has become an important matter to ensure the fundamental right 'Privacy'.

Research Question 2: Individuals consider smartphones more secure privacy-wise than computers.

Considering the usage of a smartphone as more immediate, more precise, and more shareable, and knowing that a smartphone is accessible to everyone in developed countries, self-disclosure through smartphones shall be analyzed.

Research Question 3: Privacy Actives exist in Portugal.

To understand the dimension of Privacy Actives on the sample and if they are a reality in the country, following the evidence shared in 2.3.6: Privacy, data protection, and brands' trusting.

Methodology and data collection

An online survey was designed to be shared with citizens. The survey was created in Qualtrics Analytics and is composed of the sections presented in Table 5: Structure of Questionnaire 'Perceived Impact for Citizens'.

#	Section	
1	▪ Consent	▪ Multiple Choice
6	▪ Demographic questions	▪ Age ▪ Gender ▪ Location ▪ Education ▪ Job ▪ Sector of activity
2	▪ Internet usage	▪ Frequency: Likert scale of 5 options ▪ Motives: Multiple choice
8	▪ Privacy	▪ Importance of privacy (Likert scale of 5 options; Multiple Choice) ▪ Knowledge of techniques to ensure data privacy/protection (Likert scale of 5 options) ▪ Data collection (Likert scale of 5 options, Multiple Choice) ▪ Companies and usage of data (Multiple choice)
6	▪ Privacy for smartphones	▪ Usage of a smartphone (Likert scale of 5 options) ▪ Privacy using smartphones (3 questions on a Likert scale of 5 options) ▪ Smartphone brand (open question) ▪ Block data collection from smartphone apps (Likert scale of 5 options)
20	▪ RGPD	▪ Information (Multiple Choice) ▪ Personal data (Multiple choice) ▪ Privacy Policy (Likert Scale of 5 options) ▪ Cookies (Likert Scale of 5 options, Multiple Choice) ▪ Profiling (Multiple Choice) ▪ Main changes (open question, Likert Scale of 5 options) ▪ Rights (Multiple Choice, Likert Scale of 5 options, open question)

Table 5: Structure of Questionnaire 'Perceived Impact for Citizens'

Internet Usage: two questions to understand the frequency of the Internet and tasks done on the Internet.

Privacy: questions to understand how respondents value the importance of privacy for them, the knowledge of techniques to ensure data protection, understanding on how data is collected during internet usage, from which means and methods and what kind of data is collected and for the different variety of purposes. Additionally, two questions on, from a given list, which companies treat better and worst clients' data.

Privacy for smartphones: questions to understand if respondents use the smartphone to access the Internet, privacy worries regarding smartphones, and the smartphone brand.

General Data Protection Regulation: questions to understand if the respondent knows GDPR and how the information was obtained, general questions regarding personal data, privacy policy, cookies, and profiling. Additionally, questions regarding GDPR implementation and the awareness regarding citizens' (new) rights.

Demographics: participants were asked about their age, educational level, gender, district, job, and sector of work.

The online survey was shared through Social Media and it was available between the 6th of February of 2021 and the 5th of April 2021. The total number of responses was 356 and 284 were finalized. From the complete questionnaires, the median response time was approximately 9 minutes.

From the 284 questionnaires finalized, 13 respondents did not accept the terms to participate in the questionnaire. For the following analysis, 271 responses will be considered.

Data treatment and analysis

The answers collected along with the metadata gathered were exported and the database was imported to SPSS, where variables were treated, and further analysis was performed. Participants' profile was analyzed using Excel.

Participant's profile

Of the 271 respondents, 74% as less than 45 years old, as is detailed in Figure 1: Age of participants.

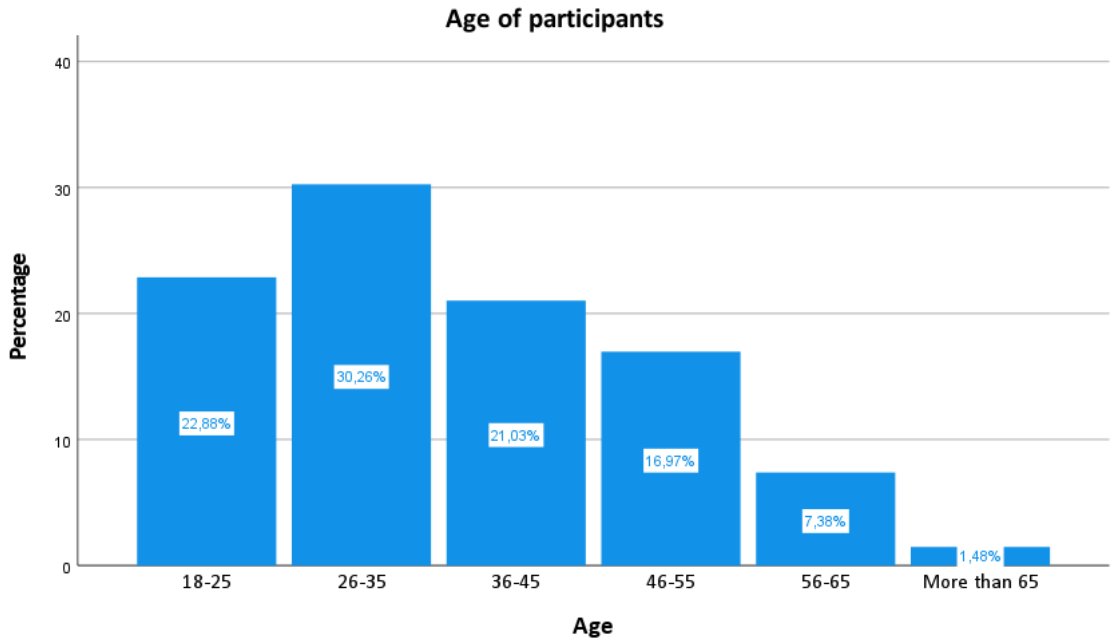

Figure 1: Age of participants

From the same sample, 72.3% are female, 27.3% are male and 1 respondent is included in the 'Other' category.

Regarding the level of education, 74% of respondents have, at least, a bachelor and 21% concluded High School.

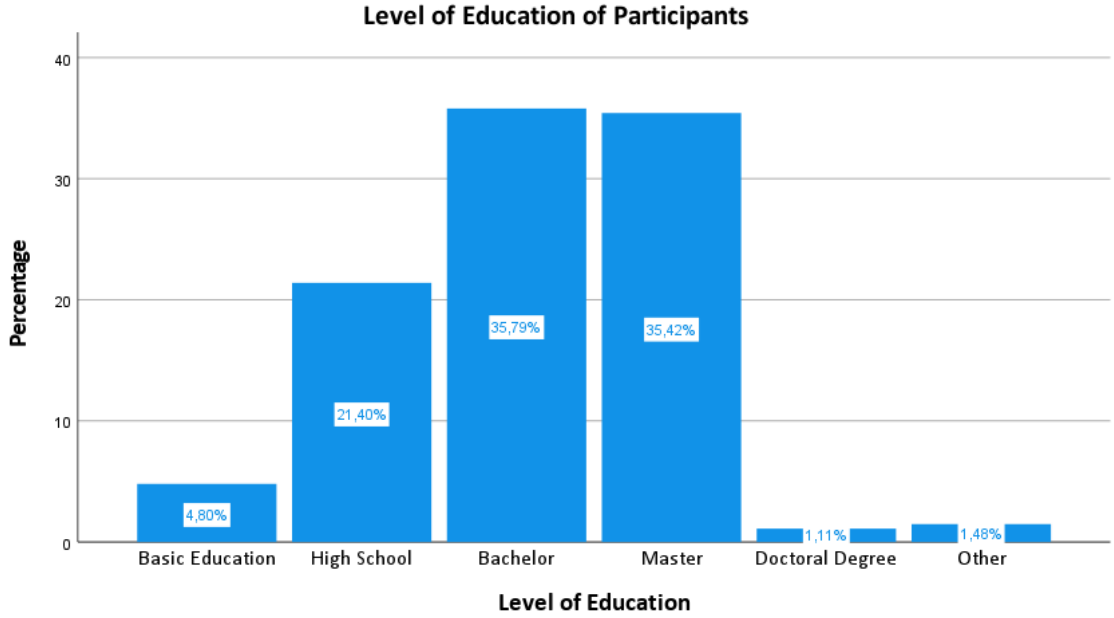

Figure 2: Level of Education of participants

Usage of Internet

Almost 98% of or respondents use the Internet daily. Respondents use the Internet to consult the e-mail (96%), use social media (95%), do searches (93%), read news (88%), listen to music (74%), online shop (73%), watch movies and series (59%), look for a job opportunity (34%), online gaming (25%) and other (work, online schooling, or everything) (14%).

Privacy

When asked if privacy is important for themselves 98% of respondents agreed. Regarding the knowledge of techniques to ensure data privacy and protection during Internet usage, more than 15% of respondents admit they did not get this knowledge and 71% of the sample responded affirmatory. Following the same group of questions, 12% of the respondents do not consider their data can be saved during internet utilization. For the respondents who consider their data can be saved, they think it is collected through Cookies (78%), GPS and tracking devices (73%), questionnaires (62%), microphones, call taps and recorders (42%), cameras, scanners or CCTV (40%), Hackers and Crackers (35%).

Inquired about which data can be collected, respondents chose information about habits (79%), website/apps utilization (78%), type of buyer (74%), information about visits based on geolocation data (45%), and information regarding worker productivity (36%).

Regarding the question about what companies can do with collected data, people responded: adapt advertisement showed to me to what I am looking for (78%), create clients' profiling (73%), adapt advertisement to the location I am (70%), send offers to the client (67%), prepare models to optimize offers to clients (64%), create models to easiness my Internet usage (61%), to sell gathered data to other companies (61%) and politics influencing (0,004%), candidates pre-screening (0,004%).

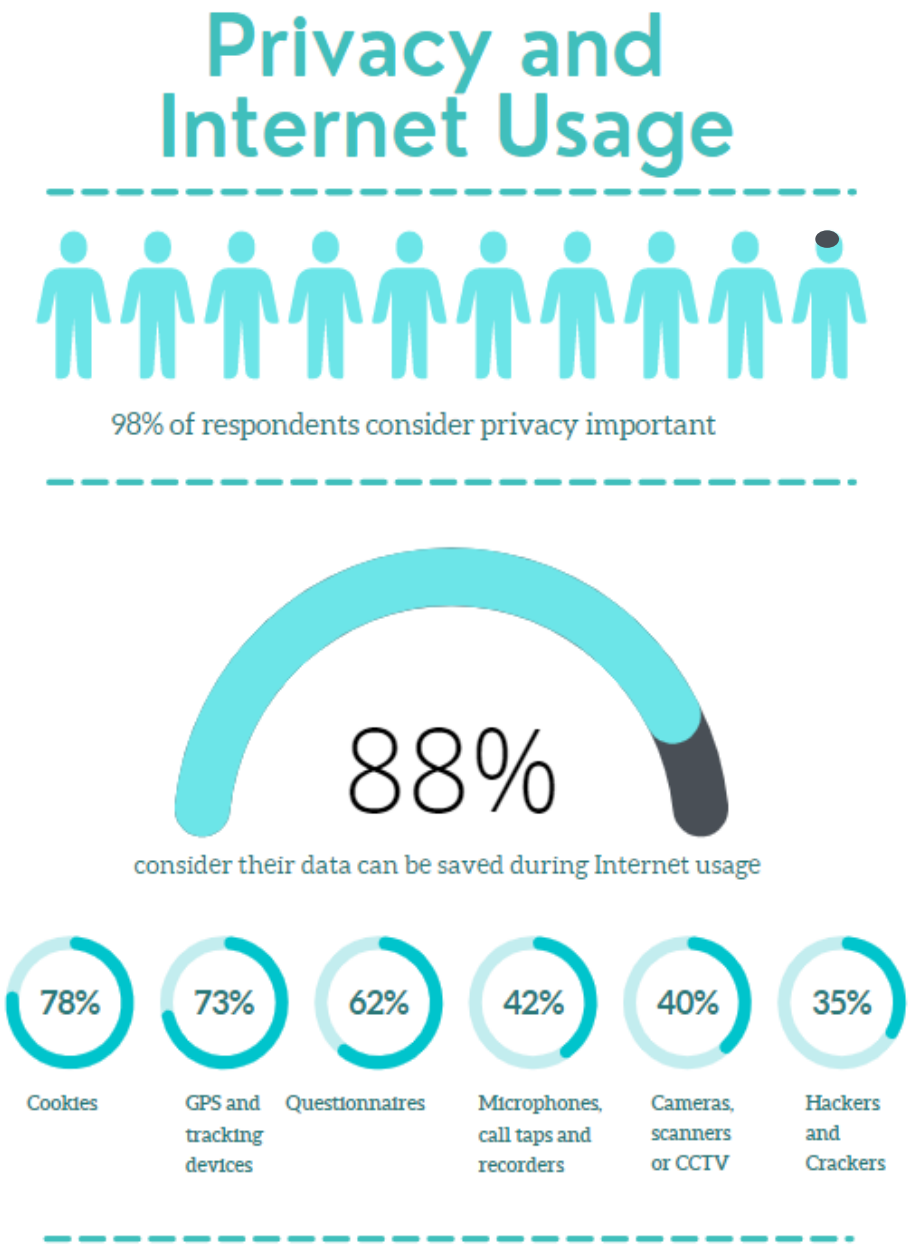

Figure 3: Infographics – Privacy and Internet Usage

After the questions regarding privacy and data collection, it was presented a list of 20 companies and respondents were asked to select the top 3 companies they consider better behave regarding data protection and which 3 have the worst behavior.

Figure 4: Top 5 companies with the best and the worst behaviors regarding data protection (respondents' opinion)

Regarding the best behavior, the top 3 is clearly settled on Microsoft (38%), Paypal (35%) and Apple (32%). Despite that, other companied were selected: Netflix (30%), Google (26%), Spotify (21%), Revolut (17%), Amazon (15%), Samsung (15%), Booking (11%), Facebook (10%), Uber (10%), HBO (6%), Huawei (5%), Xiaomi (4%), Ali Express (4%), Airbnb (4%), eBay (4%) TikTok (1%).

Regarding the worst behavior, Facebook leads the list with 198 responses (73%), followed by Google (50%) and TikTok (34%). Ali Express (31%), Booking (16%), Amazon (15%), eBay (14%), Huawei (11%), Microsoft (8%), Uber (6%), Apple (6%), Paypal (6%), Airbnb (6%), Xiaomi (6%), Netflix (4%), Samsung (2%), Spotify (2%), Revolut (3%) and HBO (1%).

Privacy and smartphones

A dedicated section to understand privacy and smartphones was developed.

When asked about the use of smartphones to access the Internet, 64% of the sample says that always use the smartphone to access the Internet and 32% use it frequently. Less than 4% use the smartphone for this effect occasionally or never.

Almost 90% of the respondents say they are worried about privacy when using their smartphones. When asked if they consider that their smartphone ensures privacy, the answers were divided: 33% believe that privacy is not guaranteed, 45% are confident that privacy is assured and 21% do not have an opinion. Additionally, 23% of respondents believe it is more secure to use the Internet through the smartphone than the computer and 43% consider the computer is securer.

The top brands of smartphones used by respondents are Apple (33%), Samsung (26%), Huawei (20%), and Xiaomi (15%). Other brands' usage is residual.

When asked if respondents try to block data collection from applications during smartphone usage, 77% refers 'Yes' and 11% 'No'.

General Data Protection Regulation

General knowledge about GDPR was also evaluated.

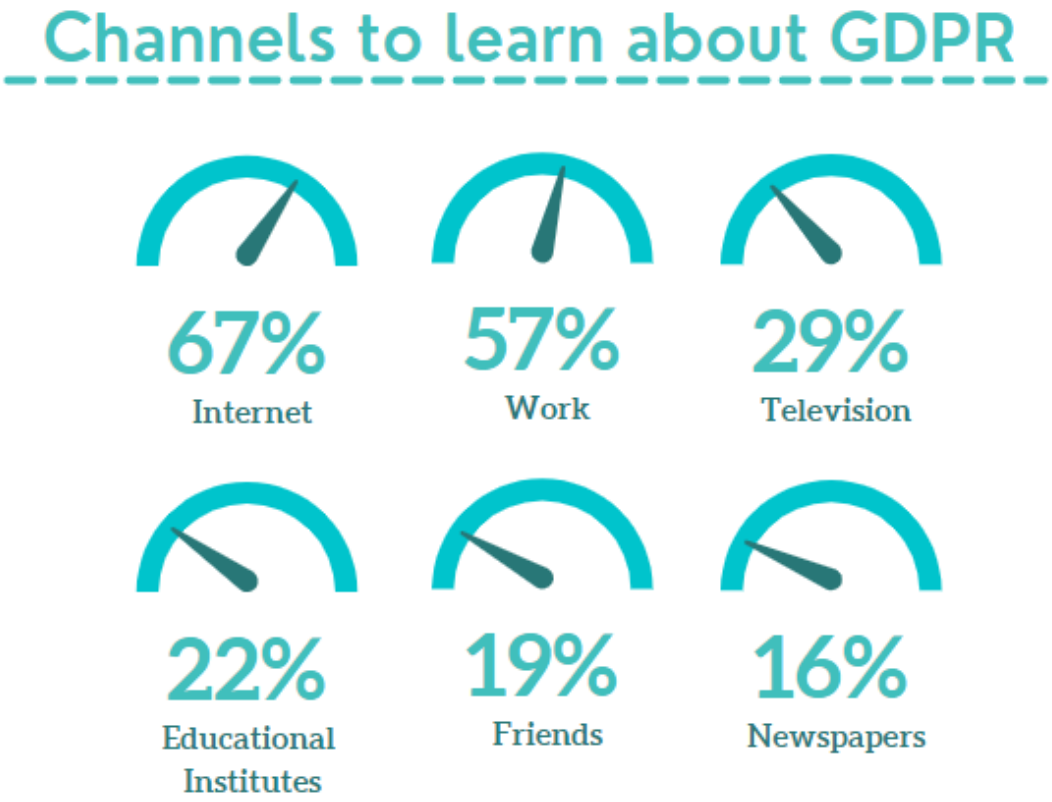

Figure 5: Channels to learn about GDPR

When asked if respondents already heard about GDPR, 94% responded affirmatively. Between a list of possible channels that could have been the source to learn about GDPR, respondents mentioned the Internet (67%), Work (57%), Television (29%), Educational Institutes (22%), Friends (19%) or Newspapers (16%). 8 persons added conversations, Republic Diary, and E-mail.

To comprehend the common understanding about personal data, people were questioned about what they consider personal data. Approximately 10% of the sample consider that only the name, e-mail, birth date, and Fiscal Number is Personal Data, while 4% added bank details to the previous data. 35% consider personal data as the previous data plus medical information and biometric data. 51% responded that personal data is everything they consider personal.

Figure 6: Privacy Police on websites

One of the main changes that were raised by GDPR was the presence of a Privacy Policy when using a website. The act of giving consent to collect and treat personal data started to be a frequent player on Internet usage. Considering that, participants were asked if they usually read this privacy policy. 8% do it frequently or always, 24% occasionally and 67% rarely or never. Despite that, 73% of respondents assumed that they accept the privacy policy all the time or most of the time. Additionally, it was asked to consider only the situations they accept the Privacy Policy and why: 78% said they accept the Privacy Policy is the only way to access the website, 17% consider they understand and agree with the Privacy Policy and 5% assumes they do not understand but it does not seem relevant for them.

Profiling or Automated Personal Data Processing is another topic brought about by the development of information and technology that GDPR tries to regulate. When asked if respondents know about the meaning of Profiling, 52% responded 'Yes' and 48% responded 'No'. From the same sample, and when asked to choose between 2 alternatives, 75% of respondents prefer to do not give access to personal data and receive advertisements less interesting than giving access to personal data and receive advertising that fits their interests (25%).

General Data Protection Regulation and its application

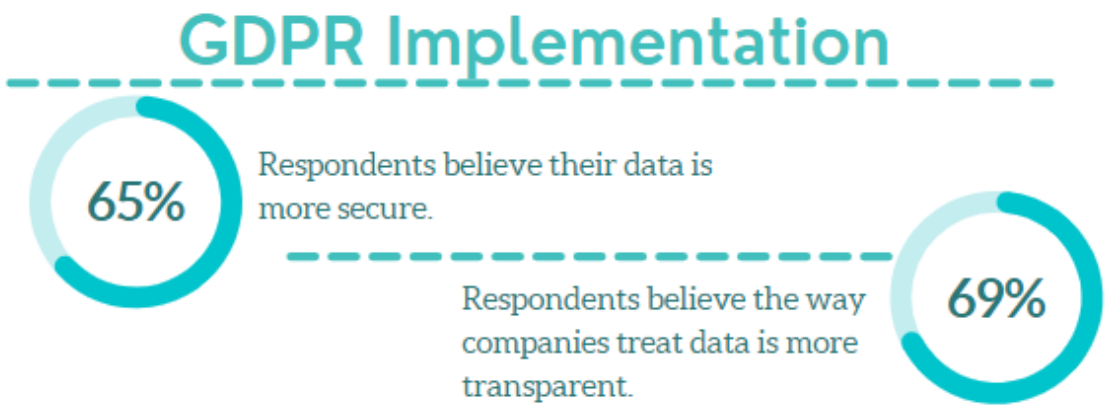

Figure 7: GDPR Implementation: security and transparency

The first question in this section was if respondents consider that their data became more secure with GDPR Implementation. 65% agree and 26% do not have an opinion. When asked if they consider that GDPR made the way companies manage their data more transparent, 69% agree and 21% do not have an opinion.

With GDPR Implementation, citizens conquer the right of asking companies that gather their data and perform different procedures, as is detailed in chapter 2.3.2: .

The rights for the data subjects. Between a list of the different possibilities, the most known was Information and Access (175), followed by Rectification and Deletion (160), Limitation of Treatment (145), Opposition to Profiling (117), and Portability (99).

80% of respondents never asked (or know someone who did it) to a company any of the previous procedures. Of the 20% that did it or know someone who did it, the most used communication channel was e-mail (57%), followed by phone call (24%). 56% of respondents considered the process easy and transparent. 67% mention that they received a response from the company in the first month and 13% never received an answer.

Summarizing the responses regarding the process:

Figure 8: GDPR and requests to companies

Procedure: 60% of the sample considered the procedure as adequate, satisfactory, or very satisfactory.

Time: 55% considered the time adequate, satisfactory, or very satisfactory and 45% were unsatisfied or very unsatisfied.

Easiness: 34% were unsatisfied or very unsatisfied with the easiness of the process. 33% consider it as 'Adequate'.

Transparency: 33% of the respondents consider it 'Adequate' and 33% were satisfied or very satisfied with the transparency during the process.

Clarity: regarding clarity, 39% of the participants considered it unsatisfactory or very unsatisfactory. 26% were satisfied or very satisfied with it.

Result: 39% of participants considered the result satisfactory or very satisfactory. 26% of the sample consider it unsatisfactory or very unsatisfactory.

Results' Discussion

Considering that the survey was shared online, the sample is composed of Internet Users who understand that their data can be collected during Internet Usage (88%).

When asked to select the brands with better and worst behaviors regarding data protection, participants demonstrated a clear position regarding the worst data protection policies: Facebook and Google, both dominant players. Google decided to eradicate third-party cookies in Chrome in 2022 and, despite the clear pros in terms of privacy, this measure will not impact the tracking of dominant platforms for Google and Facebook. (Geradin, Katsifis, & Karanikioti, 2021)

Regarding GDPR and the obligation to obtaining explicit consent, 78% said they accept the Privacy Policy because it is the only way to access the website. According to Robertson & Muirhead, (2020), the consent concept is blurry. Most consents are click-through the detailed information is not easy to comprehend.

48% of the sample do not understand what profiling is. When asked to choose between 2 alternatives, 75% of respondents prefer to do not give access to personal data and receive advertisements less interesting than giving access to personal data and receive advertising that fits their interests (25%). This contradicts the evidence that found that a large group of Europeans (75%) would choose targeted advertising than pay for a service (with a subscription) (IABEurope, 2021). This can be explained by a limitation on the available alternatives (a. Do not allow access to my personal data and receive less interesting advertisements; b. Share my personal data and receive interesting advertisement that fits what I am looking for.

Concerning the GDPR implementation, 65% of the sample believes their data is more secure and 69% believe the way their personal data is managed is more transparent.

This study aims to understand the perception of Portuguese citizens about Privacy issues and GDPR implementation.

During this work, three Research Questions were analyzed:

Research Question 1: *Do Individuals have knowledge of online privacy issues?* With the spread of online adoption around the world, benefits and negative consequences appear. Having information and comprehension about the topic is critical to ensure the benefits overlap the negative aspects.

It is important to understand if people know about the risks of their actions and channels and techniques to protect themselves.

When asked how they agree with the sentence 'Privacy is important for me', 98% agreed. However, when asked about techniques to grant data protection and privacy, more than 15% admit they do not lead them.

When asked about what personal data is, the responses were divided but only 35% answered correctly. Additionally, almost 50% of the sample did not know what profiling is, which represents a lack of knowledge on a significant method that uses their data.

Considering this sample, further investment in online privacy literacy shall be considered. The International WG on Digital Education launched a

Personal Data Protection Competency Framework for School Students that would bring positive insights to the whole population. (International WG on Digital Education, 2016)

Research Question 2: *Considering the evidence that accesses to the Internet through Smartphones is less secure than through computers, do age, level of education, or operative system of smartphones affect the perception of smartphones being more secure privacy-wise than computers.*

Smartphones were widely adopted by youngers and adult people around the planet.

Considered as an essential gadget, the ease of download an application and instantaneous start to use it can bring important issues on online privacy.

This research question aims to understand which variables may affect an individual's consideration that smartphones are more secure private-wise than using computers.

When asked if individuals are worried about privacy while using the smartphone, 90% said yes (against 98% when the question was broader). Despite that, when asked if they consider that their smartphone ensures privacy, 33% believe that privacy is not

guaranteed, and 45% are confident that privacy is assured. When inquired about by which channel is securer to access to the Internet, 23% of the sample believe it is more secure to use the Internet through the smartphone than the computer while 43% consider the computer is securer.

This deeper analysis will try to understand which variables may affect the answers to the question: I *consider that access to the internet through a smartphone is securer than through the computer.*

Given the response type chosen was a Likert Scale, the test used is the correlation of Spearman.

Hypothesis 1: Age

While undecided is the most common answer is almost all age groups (except between 26-35 years old), people tend to disagree on the sentence.

CrossTab Age * Smartphone securer

Age	Smartphone securer									
	Totally disagree		Partially disagree		Neither agree nor disagree		Partially agree		Totally agree	
	N	%	N	%	N	%	N	%	N	%
18-25	8	17.8%	18	27.7%	24	25.8%	9	21.4%	3	15.8%
26-35	15	33.3%	30	46.2%	23	24.7%	11	26.2%	3	15.8%
36-45	4	8.9%	10	15.4%	22	23.7%	10	23.8%	4	21.1%
46-54	12	26.7%	4	6.2%	16	17.2%	9	21.4%	5	26.3%
More than 56	6	13.3%	3	4.6%	8	8.6%	3	7.1%	4	21.1%
Total	45	100%	65	100%	93	100%	42	100%	19	100%

Table 6: Crosstab Age*SmartphoneSecurer

H_0: Age does not affect the perception of security privacy-wise on a smartphone.

H_1: Age affects the perception of security privacy-wise on a smartphone.

Correlation SmartphoneSecurer*Age

		Age
Smartphone Securer	Correlation coefficient	-0.07
	Sig. (2-tailed)	0.253
	N	271

Table 7: Correlation SmartphoneSecurer*Age

With a p-value of 0.252, we fail to reject H_0.

Hypothesis 2: Educational Level

The level of education of participants seems to have an impact on the answer to this question. Almost 62% of participants with Basic Education agreed with the sentence, and 37% with Secondary Education showed the same behavior.

Level of Education										
Smartphone securer	Totally disagree		Partially disagree		Neither agree nor disagree		Partially agree		Totally agree	
	N	%	N	%	N	%	N	%	N	%
Basic Education	0	0%	0	0%	5	5.4%	3	7.1%	5	26.3%
High School	7	14.2%	9	13.2%	21	22.6%	17	40.5%	4	21.1%
Bachelor	19	38.8%	22	32.3%	39	41.9%	12	28.6%	5	26.3%
Master	21	42.9%	36	52.9%	25	26.9%	10	23.8%	4	21.1%
Doctoral Degree	2	4.1%	0	0%	1	1.8%	0	0%	0	0%
Other	0	0%	1	1.4%	2	2.2%	0	0%	1	5.3%
Total	49	100%	68	100%	93	100%	42	100%	19	100%

Table 8: Crosstab LevelOfEducation*SmartphoneSecurer

H_0: Educational Level does not affect the perception of security privacy-wise on a smartphone.

H_1: Educational Level affects the perception of security privacy-wise on a smartphone.

Correlation SmartphoneSecurer*Education		
		Education
Smartphone Securer	Correlation coefficient	0.290**
	Sig. (2-tailed)	<0.001
	N	271

Table 9: Correlation LevelOfEducation*SmartphoneSecurer

Given a p-value of <0.001, H_0 is rejected.

Hypothesis 3: Operative system of the smartphone

Independently of the operative system of the smartphone, respondents were undecided (34%). People using Android are eager to respond that agree.

CrossTab Operative System * Smartphone securer						
Smartphone securer	Gender					
	Ios		Android		Total	
	N	%	N	%	N	%
Totally disagree	29	15.9%	20	22.5%	49	18.1%
Partially disagree	44	24.2%	24	27%	68	25.1%
Neither agree or disagree	64	35.2%	29	32.6%	93	34.3%
Partially agree	30	16.5%	12	13.5%	42	15.5%
Totally agree	15	8.2%	4	4.5%	19	7%
Total	182	100%	89	100%	271	100%

Table 10: Crosstab OperativeSystem*SmartphoneSecurer

H_0: Operative System of Smartphone does not affect the perception of security privacy-wise on a smartphone.

H_1: Operative System of Smartphone affects the perception of security privacy-wise on a smartphone.

Correlation SmartphoneSecurer*OperativeSystem		
		Education
Smartphone Securer	Correlation coefficient	0.106
	Sig. (2-tailed)	0.082
	N	271

Table 11: Correlation SmartphoneSecurer*OperativeSystem

Given a p-value of 0.082, we fail to reject H_0.

With the performed tests, we may reject the null hypothesis that Educational Level does not affect the response. There is not any correlation between the sense of SmartphoneSecurer and Age or Operative System.

Research Question 3: Privacy Actives exist in Portugal.

The Privacy Actives, as explained in 2.3.6: Privacy, data protection, and brands' trusting are people that value privacy and is available to fight for it against companies (Cisco Secure, 2020)

Considering the answers given to the question *'Do you value privacy while using a smartphone' and 'Have you ever (or did you know someone) who use one of the rights brought by GDPR?',* 18% of the sample is a Privacy Active.

From this group, approximately 80% has less than 45 years old and 80% completed, at least, a Bachelor.

Any of the mentioned variables impacts the probability of being a Privacy Active, as can be seen in the next table that contains a Spearman Correlation between Being Privacy Active and the mentioned aspects (there are no p-values below 0.05).

Correlation PrivacyActive		
		PrivacyActive
Age	Correlation coefficient	-0.024
	Sig. (2-tailed)	0.689
	N	271
Level of Education	Correlation coefficient	0.021
	Sig. (2-tailed)	0.732
	N	271
Smartphone Operative System	Correlation coefficient	-0.063
	Sig. (2-tailed)	0.3
	N	271

Table 12: Correlation PrivacyActive*Age, Level of Education and Smartphone Operative System

3.1.2. Privacy paradox: the usage of StayAway Covid application

In 2019, a global pandemic brought an exceptional challenge to the world.

COVID-19 (Coronavirus disease) was firstly reported by the People's Republic of China government, on 31 December of 2019, as viral pneumonia, but rapidly was spread in the world. Being highly contagious and giving serious consequences to some of the patients infected, the world is joining efforts to control it.[2]

To control the spreading of the virus, governments and health authorities advise people to keep social distancing and start to improve ways of identifying, evaluate, and manage people exposed to the disease, naming this process as Contact Tracing. If well applied, contact tracing helps to keep the normal routine of families and business, once people exposed is isolated. (WHO, 2020) (Jonker et al., 2020)

Jonker et al. (2020) report the workload as one of the disadvantages of contact tracing measures: having in mind that exposed people shall be rapidly identified and informed, manual, and time-consuming processes can cause delays and consequently, a reduction in process' effectiveness. Retrieving the benefits of facing a global pandemic during the digitalization era, different governments adopted Digital contact tracing (DCT) apps, that pretend to easily send notifications of exposure to the app users that faced a risky contact.

These apps use location data, that can be categorized into two types: absolute location data (GPS-based) and relative location data (Bluetooth-based). The decision of the technology used, and its effectiveness can be influenced by precision and security matters. While relative location data seems to be more precise, it is needed to have a significant portion of the population using it to be effective. Absolute location data is constantly collected while relative location data is only collected while people if the application is installed and activated. Regarding security, Tang (2020) refers to two concerns: data authenticity and privacy. While absolute location data looks more

[2] Source: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/coronavirus-disease-covid-19 (accessed at 08/02/2021)

authentic (it can be confirmed by a third party), it represents a higher level of concern in privacy regards if disclosed. (Blasimme & Vayena, 2020) (Tang, 2020)

The Portuguese government and Portuguese Health Authorities followed the global trend of DCT, and the app StayAway Covid was developed. The development oversaw the Institute for Systems and Computer Engineering, Technology and Science (INESC TEC), Institute of Public Health of the University of Porto (ISPUP), supported by two companies (Keyruptive and Ubirider). Foundation for Science and Technology (FCT) operates and maintains the system and assumes the role of the data controller. A Data Protection Impact Assessment (DPIA), a prior consideration by the Portuguese Data Protection Authority (CNPD), and an audit developed by the Portuguese National Cybersecurity Centre were established to ensure the security of the system. (INESCTEC, 2020)

STAYAWAY COVID has free and public access, and its download and usage are completely voluntary. The personal data treated by STAYWAY COVID System are resumed in Table 13: Personal data treated by STAYAWAY SYSTEM (INESCTEC, 2020).

Type of data	Detail of data	Storage
Pseudonymized data	TEK Identifier Keys and Random RPI Identifiers	14 days after storage
Pseudonymized data	Universal Unique Identifier	Deleted during daily database maintenance task (max 24 hours)
Health data	TEK Identifier Keys shared after diagnosis	14 days after storage
Health data	▪ Contact information: date, duration, and estimated distance of contact	14 days after storage
Health data	▪ Date of first symptoms ▪ Test date for asymptomatic patients	Deleted during daily database maintenance task (max 24 hours)
IP Address	IP address	No longer than one hour

Table 13: Personal data treated by STAYAWAY SYSTEM (INESCTEC, 2020)

According to Data Report (2020), in January 2020, 7.82 million Portuguese people were mobile internet users, and 93% own a smartphone.

STAYAWAY COVID app was downloaded about 3.05 million times between September 2020 and the 10th of February 2021, according to the data shared by INESC TEC. The evolution of downloads of the application is described in Figure 9: Cumulative number of downloads of StayAway Covid app, between the 1st of September 2020 and the 10th of February 2021. (Source: INESC TEC with data from official stores)**Error! Reference source not found.**).[3]

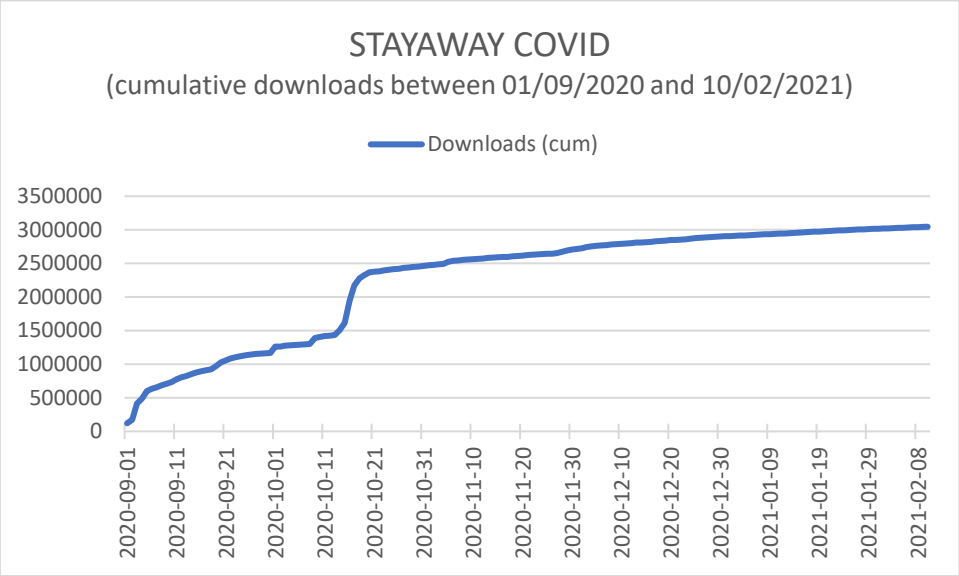

Figure 9: Cumulative number of downloads of StayAway Covid app, between the 1st of September 2020 and the 10th of February 2021. (Source: INESC TEC with data from official stores)

The peak of active users was achieved on 19 October, with more than 1.75 million active users. The total number of active users on 13 January of 2021 was 1.15 million, less than 40% of the sum of the downloads.[4]

[3] Data shared by INESC TEC at 11/02/2021

[4] Source: https://www.publico.pt/2021/01/15/tecnologia/noticia/60-ja-apagaram-stayaway-covid-sao-18-milhoes-portugueses-1946366 (accessed at 08/02/2021)

A recent study about the impact of different levels of adoption of DCT apps concludes that compared with the default option of not having a digital exposure app, benefits were found for all levels of app adoption. (Abueg et al., 2020)

Besides that, the STAYAWAY-COVID system was not widely proliferated (if all downloaded apps were kept active, we would have less than 40% of Portuguese people with a smartphone using the app), despite the overall efforts to ensure privacy on its usage and Portuguese Authorities attempts to conquer users and its trust.

This scenario is common to other countries: only 13,4% of Italians, 24% in Irish and 19,3% of Germans installed their countries' app (Blasimme & Vayena, 2020)

A survey conducted in July in the UK concluded that people between 18-25 say they would download the app while the oldest age groups (65+) have fewer people interested. Respondents in professional, administrative, and management roles say more they would download the app, and people with no formal education would download it less than the overall (Ipsos MORI, 2020)

According to Tang (2020), one of the reasons pointed as a concern of DCT apps is related to authenticity and privacy tradeoffs. Additionally, in Portugal, bureaucracy aspects seem to help the proliferation of an idea of a useless application.

A study conducted online on Facebook users of active age (18-65) aims to test the paradox of privacy, using a use case focused on STAYAWAY COVID Application and its usage.

The study aims to answer the following Hypothesis:

Hypothesis 1*:* Concerns about privacy issues affect the adoption of applications that help to answer other problems.

Hypothesis 2: Age affects fears regarding privacy.

Hypothesis 3: Level of education affects fears regarding privacy.

Methodology and data collection

A scenario where public health is at risk might be useful to test if people are effectively concerned about privacy or if the level of concern about privacy can change depending on the conditions and the value we attribute to different variables.

To collect data, a 5 minutes-survey was designed to be shared online, with multiple choice and open questions. The survey was created in Qualtrics and is composed of the sections presented in Table 14: Structure of Questionnaire 'StayAway Covid'.

#	Section	
1	▪ Consent	▪ Multiple Choice
2	▪ Measure to control the pandemic in Portugal	▪ Perceived impact of restrictions taken to control the proliferation of Covid in Portugal (Likert Scale of 5 options)
7	▪ StayAway Covid	▪ Application usage (Likert Scale of 5 options) ▪ Preferences (Multiple choice) ▪ Open questions to understand previous answers
2	▪ Usage of DCT app	▪ Usage of app ▪ Open question to explain the answer
6	▪ Demographic questions	▪ Age ▪ Gender ▪ Education ▪ Job ▪ Sector of activity ▪ District of residence

Table 14: Structure of Questionnaire 'StayAway Covid'

Measures to control the pandemic in Portugal. Two questions were designed to understand the opinion of respondents about a) the group of measures taken in Portugal to control the pandemic; b) the weight on the daily routine of these measures.

STAYAWAY COVID. One question to clarify if the respondent would voluntarily use the app and if the answer were 'maybe', 'probably not' or 'certainly not', a second question is displayed, presenting multiple justifications and 'Other', where an open answer can be added.

A third question related to the usage of the app aims to understand the motivation to use the app.

The fourth and fifth questions ask the respondent if, in a case of a diagnosis of COVID-19, he will mark him as infected in the app and why.

The sixth question aims to understand the perception of risk using the app.

The last question of this section encourages respondents to prioritize privacy and public health.

Usage. This section contains two questions, to understand if the respondent uses STAYAWAY COVID App and why.

Demographics. In the last section, participants were asked about their age, educational level, gender, district, job, and sector of work.

The online survey was shared through Facebook and was available between 22 December 2020 and the 4th of January 2021. The medium duration of answers was around 6 minutes.

Data treatment and analysis

The answers collected along with the metadata gathered were exported to a CSV file and treated using Excel. Basic data description was developed in Excel.

Then, the database was imported to SPSS, variables were treated, and further analysis was performed.

Participants' profile

Considering that the privacy paradox refers to the desire for self-disclosure while claiming for privacy (Taddicken, 2014), the survey was randomly shared between Facebook users, to ensure that all the participants were social media consumers.

Of the one hundred and forty-six participants, 79% successfully finished the survey (n=115).

Of the respondents, 33 (31%) are male and 79 (69%) are female. 60% has less than 34 years old (deeper representation at Figure 10: Age range of survey participants) and all of them are residents in Portugal.

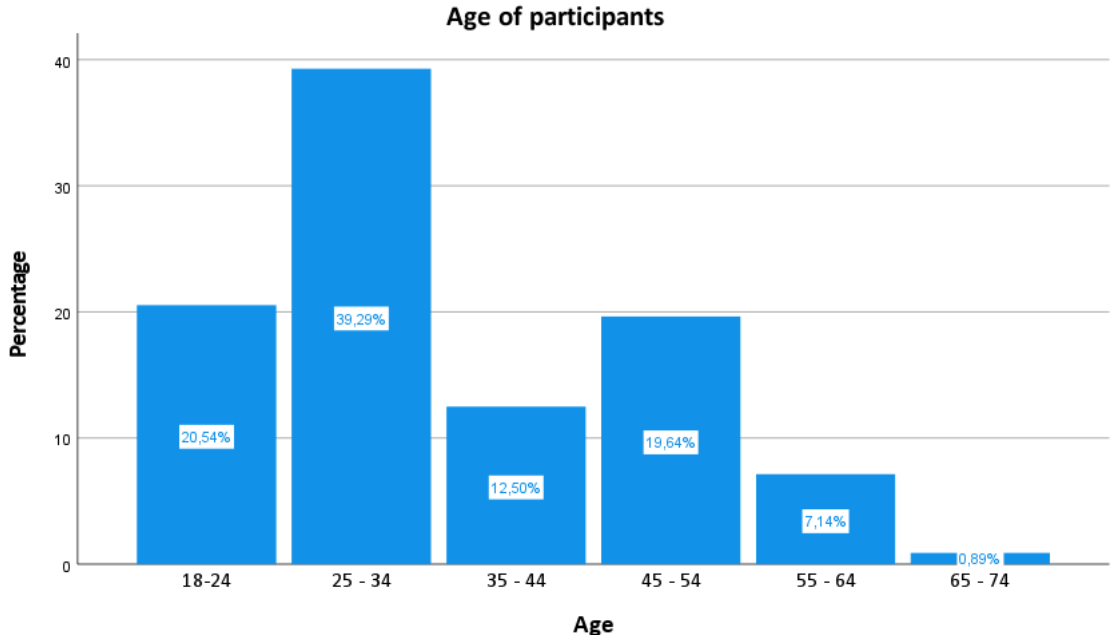

Figure 10: Age range of survey participants

Regarding the educational background, 68% completed higher education, as detailed in Figure 11: Academic Background of participants.

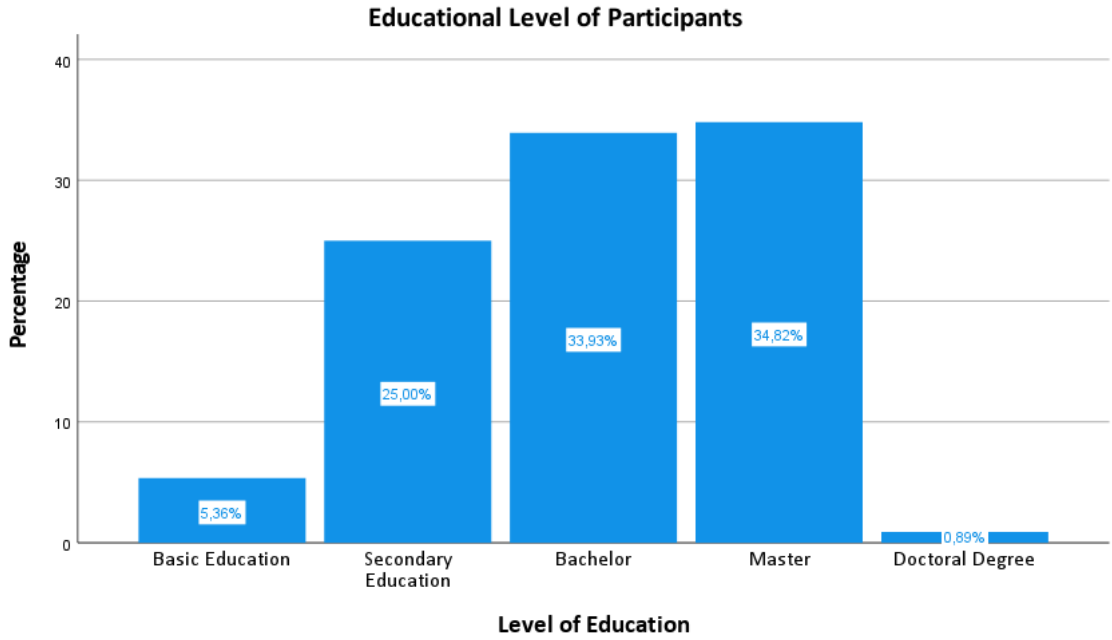

Figure 11: Academic Background of participants

Regarding the sector of work, the sectors with more frequency were Education and Finance, economics, or management.

Measures to control the pandemic in Portugal

During the pandemic, many measures were taken to control it.

To understand the perception of respondents about the measures applied, they were asked about the suitability of measures and their impact on the daily routines of their appliance.

Regarding the suitability of measures, approximately 85% of the respondents answered that the measures were partially suitable (69,64%) or extremely suitable (14,29%), as shown in Figure 12: Suitability of measures.

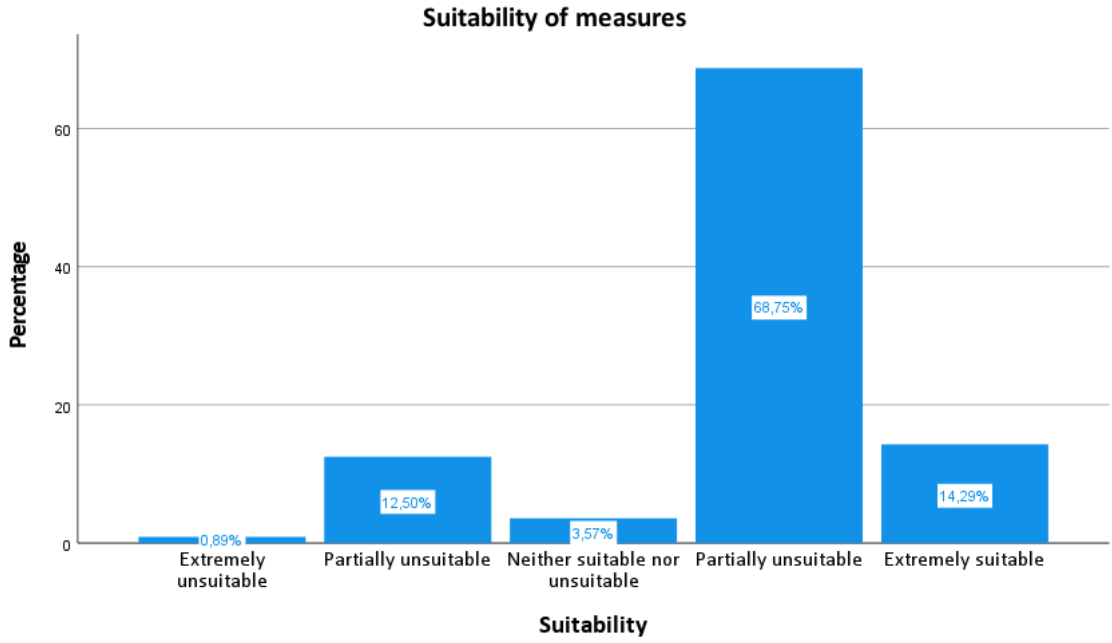

Figure 12: Suitability of measures

Concerning the weight of these measures on the daily routine, 34% of respondents believes the impact was partially excessive and approximately 52% do not consider excessive nor insufficient, as presented on Figure 13: Weight of measures on daily routine.

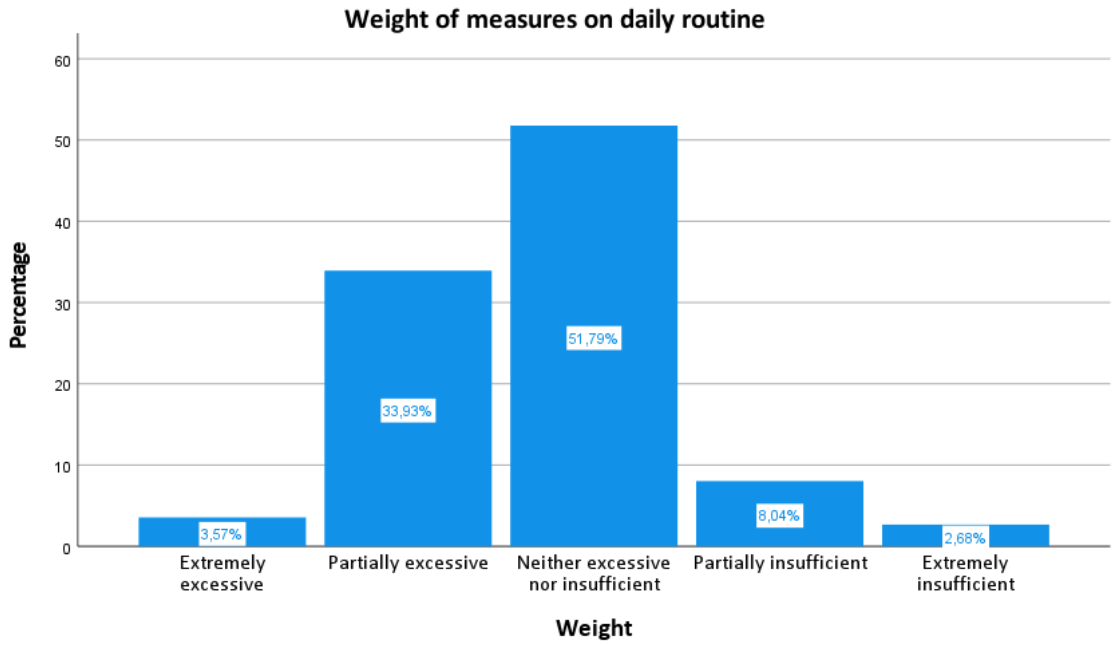

Figure 13: Weight of measures on daily routine

Use of StayAway Covid

Regarding the voluntary use of the app, from the 112 respondents, 57% would use freely the app. Of the remaining 43%, 12% did not make a decision, 13% would probably not install the app and 18% would certainly not install the app, as shown in Figure 14: Voluntary Usage of App.

To understand the reason why people did not yet decide or decided to not use it, the main answers were: do not know how the data collected is going to be treated (14), doubts about the efficacy of this type of contacts' tracing (7), prefer to wait for more tests (8) and concerns regarding the sharing of localization data (6).

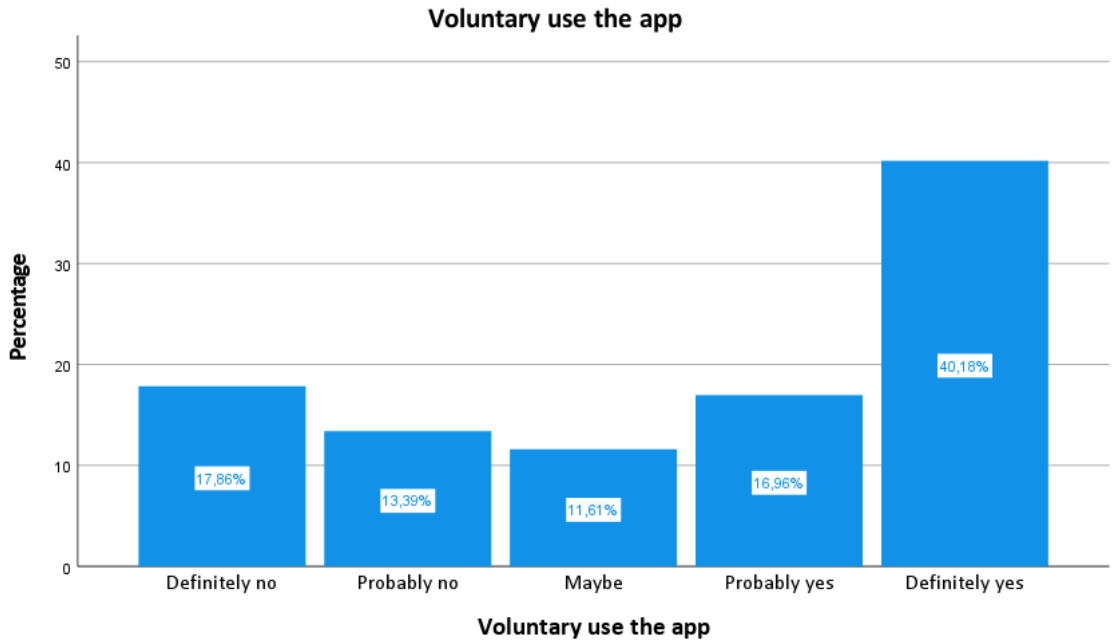

Figure 14: Voluntary Usage of App

When participants were asked about the hypothesis of register a positive diagnosis for Covid-19, 88% would probably register it through the app and about 9% would probably not register it. Asked about the motives for not register the diagnostic, respondents referred to lack of responsibility on share this information, app utility and reliability, and privacy/data treatment.

StayAway Covid and Privacy

'The usage of an application for Contact Tracing puts my privacy and/or the protection of my personal data at risk.'

Participants were asked about their level of agreement with the previous sentence. From the 112 responses, 33,9% partially or totally disagree, 22,3% neither agree nor disagree and 43,8% partially or totally agree.

Regarding the request to prioritize privacy and public health, 49,1% believe both are important, 41,1% believe public health is more important than privacy and 9,8% consider privacy more important.

Results' Discussion

***Hypothesis 1**: Concerns about privacy issues affect the adoption of applications*

The Application Programming Interface (API), developed by Google and Apple at the beginning of the pandemic, was shared with Governments of several countries to be the basis of national's contact tracing app. The usage of this API was under several conditions, being the free using one of the most communicated in Portugal.

Considered the pros and cons of Contact Tracing apps, several motivations were shared regarding the adoption of Contact Tracing apps, being privacy issues frequently addressed. It is expected that the doubts regarding the security of the Contact Tracing app negatively affect the willingness to freely use it.

To answer this research question, the voluntary adoption of a Contact Tracing app and the privacy concerns were considered. Both questions were made on a Likert Scale of 5 levels. The confidence interval considered is 95%.

H_0 = concerns about losing privacy do not affect the adoption of applications

H_1 = concerns about losing privacy affect the adoption of applications

CrossTab LossPrivacy * VoluntaryUse

LossPrivacy	VoluntaryUse									
	Definitely No		Probably No		Maybe		Probably yes		Definitely Yes	
	N	%	N	%	N	%	N	%	N	%
Totally disagree	3	15.0%	0	0.0%	2	15.4%	3	15.8%	19	42.2%
Partially disagree	1	5.0%	1	6.7%	0	0.0%	2	10.5%	7	15.6%
Neither agree nor disagree	3	15.0%	4	26.7%	5	38.5%	7	36.8%	6	13.3%
Partially agree	6	30.0%	7	46.7%	2	15.4%	7	36.8%	7	15.6%
Totally agree	7	35.0%	3	20.0%	4	30.8%	0	0.0%	6	13.3%
Total	20	100%	15	100%	13	100%	19	100%	45	100%

Table 15: Crosstab VoluntaryUse * LossPrivacy

To test the null hypothesis, a Spearman correlation test was performed.

Correlation LossPrivacy * VoluntaryUse		
		Loss Privacy
Voluntary Use	Correlation coefficient	-0.375**
	Sig. (2-tailed)	<0.001
	N	112

Table 16: Correlation between fear of losing privacy and Voluntary usage of Contact Tracing Apps.

The p-value < 0.001 suggests that the correlation is significative and H0 is rejected.

Figure 15: Privacy issues and contact tracing apps

The adoption of applications is affected by concerns related to privacy issues. In this case, the trust regarding privacy affects positively the adoption of the application: from the respondents that Partially or Totally Disagree that the usage of contact tracing brings privacy issues (n=38), 82% would probably or definitely use the app voluntarily. On the other hand, from the participants that Partially or Totally Agree that this usage may raise privacy issues (n=49), 47% would probably or definitely not use a contact tracing app voluntarily and 41% would probably or definitely use the app. From this sample, we can conclude that people that do not trust the app do not follow a clear path (like people that trust it).

Hypothesis 2: *The fear of losing privacy when using Contact Tracing Apps is affected by age*

As shared in 2.2.2: Privacy in the modern world, generational perspectives may impact the intention to self-disclosure due to a lack of knowledge on privacy issues.

This research question intends to analyze if age impacts the answers about the perception of missing privacy when using Contact Tracing Apps.

H0: Age does not affect the intention to use the app.

H1: Age affects the intention to use the app due.

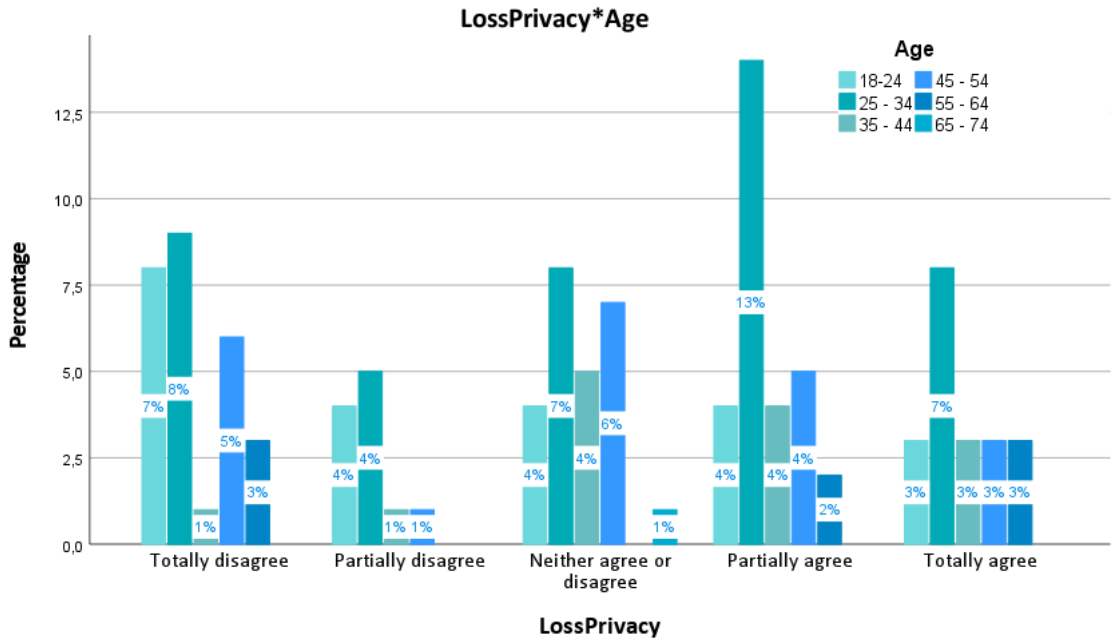

Figure 16: LossPrivacy * Age Bar chart

To analyze the null hypothesis, a Spearman correlation was tested. The results are detailed in the following table:

Correlation LossPrivacy * Age and VoluntaryUse*Age		
		Age
LossPrivacy	Correlation coefficient	0.102
	Sig. (2-tailed)	0.286
	N	112
VoluntaryUse	Correlation coefficient	0.052
	Sig. (2-tailed)	0.587
	N	112

Table 17: Correlation between Age*LossPrivacy and Age*VoluntaryUse

With a p-value of 0.286 for LossPrivacy*Age and 0.587 for VoluntaryUse*Age, we fail to reject H_0: does not exist a significant relationship between the perception of losing privacy with using these kinds of applications and the age.

Hypothesis 3: *Level of education affects fears regarding privacy.*

The perception that different levels of education may affect the assessment of risks regarding privacy issues is tested here.

H0: Level of Education does not affect the intention to use the app due to fear of losing privacy.

H1: Level of Education affects the intention to use the app due to fear of losing privacy.

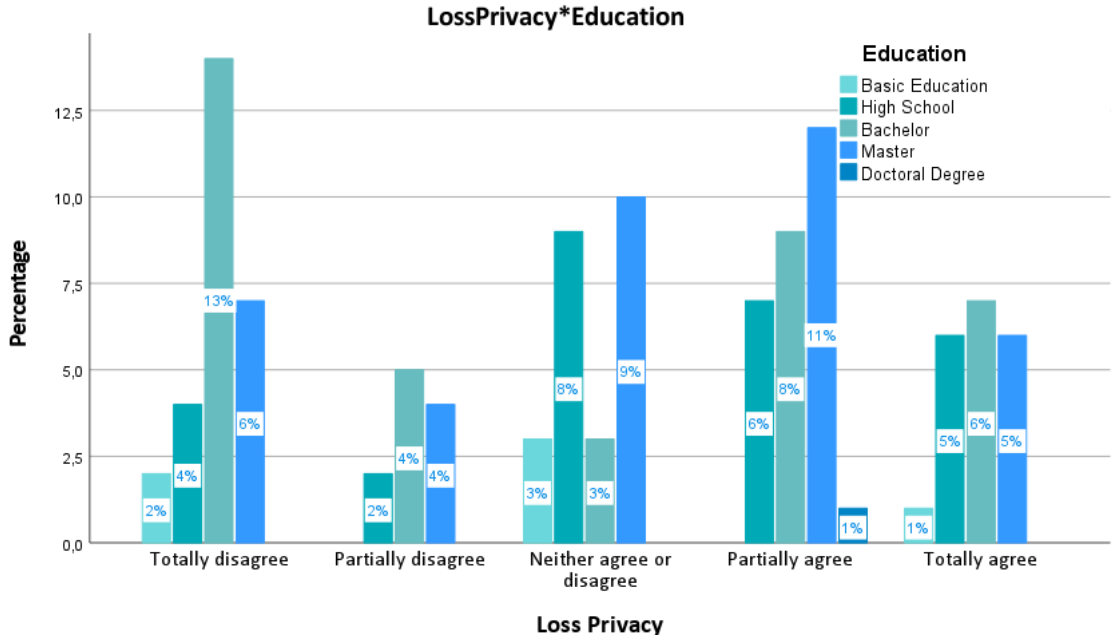

Figure 17: LossPrivacy*Education bar chart

Correlation LossPrivacy * Education and VoluntaryUse*Education		
		Education
LossPrivacy	Correlation coefficient	0.020
	Sig. (2-tailed)	0.838
	N	112
VoluntaryUse	Correlation coefficient	0.028
	Sig. (2-tailed)	0.770
	N	112

Table 18: Correlation LossPrivacy * Education and VoluntaryUse*Education

With a p-value of 0.838 for LossPrivacy*Education and 0.770 for VoluntaryUse*Education, we fail to reject H_0: does not exist a significant relationship between the perception of losing privacy with using these kinds of applications and the level of education.

4. CONCLUSION

In this study, an analysis of the perception of citizens about privacy and data protection was developed.

This work was performed to answer the following research questions, supported by the literature.

Research Question 1: Individuals have literacy on online privacy issues.

Research Question 2: Individuals consider smartphones more secure privacy-wise than computers.

Research Question 3: Privacy Actives exist in Portugal.

The existence of Privacy Actives in Portugal is true, and the other Research Questions were not proved.

Regarding literacy, this analysis let clear that there is a lack of understanding of this important thematic. Despite being an objective of GDPR, the process is not transparent to the citizens (for example, the responses about accepting privacy policy because it is the only way to access the website).

This study was relevant to understand how people in Portugal perceive the GDPR implementation, after 2-years.

Additionally, the section about Contact Tracing Apps to help to control the pandemic helped us to understand that fears and less trusted solutions may block future implementation that – used in mass – could bring benefits to the entire country.

Privacy has been acquiring importance over the years. Companies can collect and treat, more than a high amount of data, more precisely. The path of having 'Data-Driven Decisions', both for Business and Marketing, bringing companies countless benefits and improvements.

Given that the power comes with responsibilities, the way companies treat customers' data may represent the way they treat customers and constitute a risk to their brands.

GDPR raises the interest in the topic and citizens are responding to the challenge, staying more attentive and predictive.

While some consumers are trying to recover their control regarding their data, there is a lack of knowledge on online privacy issues and protection. Being education the basis of progress, governments shall invest on create awareness for this problem.

From my understanding, we shall not block digital improvements: they can bring us countless solutions and benefits. Despite that, it is important to battle for a boundary where security and privacy are assured. In an increasingly digital society, we shall educate and create awareness, never delay, or block.

4.1. Limitations

The main limitation of this study is the lack of studies on the same topic and population. This gave me additional challenges due to the inexistence of literature to validate my hypothesis.

Given that, this study is a descriptive analysis of the data acquired through the questionnaires.

4.2. Recommendations for future work

Despite the need of having a bigger group of participants, I would suggest having a focus group instead of an online survey.

Study deeply Privacy Actives would bring companies more information about this new type of profile.

Another recommendation is to bring companies to the discussion and analysis, performing some individual interviews with different stakeholders and understand their perceptions and challenges.

5. REFERENCES

Abueg, M., Hinch, R., Wu, N., Liu, L., Probert, W., Wu, A., … Fraser, C. (2020). Modeling the combined effect of digital exposure notification and non-pharmaceutical interventions on the COVID-19 epidemic in Washington state. *MedRxiv*. https://doi.org/10.1101/2020.08.29.20184135

Aditya, P., Bhattacharjee, B., Druschel, P., Erdélyi, V., & Lentz, M. (2014). Brave new world: Privacy risks for mobile users. *SPME 2014 - Proceedings of the ACM MobiCom Workshop on Security and Privacy in Mobile Environments*, 7–11. https://doi.org/10.1145/2646584.2646585

Armando, C., Netto, A., Cássia, C., Abilio, C., Maria, S., Coutinho, V., … Lago, M. (2019). *A Janela de Johari como ferramenta de análise da privacidade de dados pessoais*. 79–93.

Asthon, K. (2010). That ’ Internet of Things ’ Thing. *RFID Journal*, 4986. https://doi.org/10.1038/nature03475

Atzori, L., Iera, A., & Morabito, G. (2014). From “smart objects” to “social objects”: The next evolutionary step of the internet of things. *IEEE Communications Magazine*, *52*(1), 97–105. https://doi.org/10.1109/MCOM.2014.6710070

Austin, L. (2002). *Privacy and the question of technology*. (September 2002), 119–166.

Beckett, P. (2018). GDPR compliance: your tech department’s next big opportunity. *Computer Fraud & Security Bulletin*, *2017*(5), 9–13. https://doi.org/10.1016/S1361-3723(17)30041-6

Benfenatki, H., Goncalves, L., Nicolas, O., Winckler, M., & Bernard, U. C. (2018). *Towards a User Centric Personal Data Protection Framework*. (May).

Bhat, A. (2019). Quantitative Research Methods.

Blasimme, A., & Vayena, E. (2020). What’s next for COVID-19 apps? Governance and oversight. *Science*, *370*(6518), 760–762. https://doi.org/10.1126/science.abd9006

Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, *37*(3), 466–480. https://doi.org/10.1016/j.ijresmar.2020.03.006

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online Behavioral

Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, *46*(3), 363–376. https://doi.org/10.1080/00913367.2017.1339368

Boyd, D. (2007). Social Network Sites: Public, Private, or What ? Social Network Sites Mediated Publics. *Knowledge Tree*, 1–7. https://doi.org/10.4018/jantti.2010040104

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Carter, P., Laurie, G. T., & Dixon-woods, M. (2015). *The social licence for research: why care data ran into trouble*. 404–409. https://doi.org/10.1136/medethics-2014-102374

Cisco Secure. (2020). *Protecting Data Privacy to Maintain Digital Trust*.

Cooley, T. M. (1879). *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract* (Vol. 1). https://doi.org/10.2307/823885

Data Report. (2020). *Digital 2020 - Portugal*. Retrieved from https://datareportal.com/reports/digital-2020-portugal

DeCew, J. W. (2016). Privacy and Its Importance with Advancing Technology. *O Northern University Law Review*, *42*(471), 471–492. https://doi.org/10.3366/ajicl.2011.0005

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). *We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy*. (February). https://doi.org/10.14722/ndss.2019.23378

Dias, C. A. (2005). Hipertexto: evolução histórica e efeitos sociais. *Ciência Da Informação*, *28*(3), 269–277. https://doi.org/10.1590/s0100-19651999000300004

Drucker, E. P. (1999). The Evolution of Internet Genres. *Computers and Composition*, *16*, 269–282.

European Commission. (2019). Internet of Things - Brochure. Retrieved July 12, 2020, from https://ec.europa.eu/digital-single-market/en/news/internet-things-brochure

European Union. (2012). Tratado sobre o Funcionamento da União Europeia (Versão Consolidada). *Jornal Oficial Da União Europeia*, 47–390.

Facebook: Terms and Conditions. (2020). Retrieved January 17, 2020, from https://www.facebook.com/legal/terms/update

Floridi, L. (2005). Is Semantic Information Meaningful Data? *Philosophy and Phenomenological Research*, *70*(2), 351–370. https://doi.org/10.1111/j.1933-1592.2005.tb00531.x

Furini, M., Mirri, S., Montangero, M., & Prandi, C. (2020). Privacy Perception when Using Smartphone Applications. *Mobile Networks and Applications*, *25*(3), 1055–1061. https://doi.org/10.1007/s11036-020-01529-z

GDPR. (2016). General Data Protection Regulation. *Official Journal of the European Communities*, *2014*(March 2014), 1–88. https://doi.org/http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf

Geradin, D., Katsifis, D., & Karanikioti, T. (2021). Google as a de facto privacy regulator: analysing the Privacy Sandbox from an antitrust perspective. *European Competition Journal*, *0*(0), 1–65. https://doi.org/10.1080/17441056.2021.1930450

Hargittai, E., & Marwick, A. (2016). "What can i really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757. https://doi.org/10.5167/uzh-148157

IABEurope. (2021). *WHAT WOULD AN INTERNET WITHOUT TARGETED ADS*.

Ibarra-Esquer, J. E., González-Navarro, F. F., Flores-Rios, B. L., Burtseva, L., & Astorga-Vargas, M. A. (2017). Tracking the evolution of the internet of things concept across different application domains. *Sensors (Switzerland)*, *17*(6), 1–24. https://doi.org/10.3390/s17061379

INESCTEC. (2020). STAYAWAY COVID. Retrieved February 8, 2021, from https://stayawaycovid.pt/

International Data Corporation. (2019). The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast. Retrieved July 12, 2020, from https://www.idc.com/getdoc.jsp?containerId=prUS45213219

International WG on Digital Education. (2016). *Personal Data Protection Competency Framework for School Students*. (October), 1–16.

Ipsos MORI, P. A. (2020). *The Health Foundation COVID-19 Survey – second poll*. (July).

ITU. (2005). ITU Internet Reports. The Internet of Things. *International Telecommunication Union*, 212. https://doi.org/10.2139/ssrn.2324902

Jonker, M., de Bekker-Grob, E., Veldwijk, J., Goossens, L., Bour, S., & Mölken, M. R. Van. (2020). COVID-19 contact tracing apps: Predicted uptake in the Netherlands based on a discrete choice experiment. *JMIR MHealth and UHealth*, *8*(10), 1–14. https://doi.org/10.2196/20741

Laudon, K. C., & Traver, C. G. (2014). *E-Commerce*.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., … Wolff, S. (2009). A brief history of the Internet and the World Wide Web. In *ACM SIGCOMM Computer Communication Review* (pp. 15–24).

Madden, M., Lenhart, A., Cortesi, S., & Gasser, U. (2013). Teens and mobile apps privacy. Retrieved February 7, 2021, from Washington, DC: Pew Research Center. website: https://www.pewresearch.org/internet/2013/08/22/teens-and-mobile-apps-privacy/

Mag, T. J. (2011). Fourteen reasons privacy matters: A multidisciplinary review of scholarly literature. *Library Quarterly*, *81*(2), 187–209. https://doi.org/10.1086/658870

Mannhardt, F., Petersen, S. A., & Oliveira, M. F. (2018). Privacy Challenges for Process Mining in Human-Centered Industrial Environments. *Proceedings - 2018 International Conference on Intelligent Environments, IE 2018*, 64–71. https://doi.org/10.1109/IE.2018.00017

Mark, J., Rumbold, M., & Chb, M. B. (2017). *The Effect of the General Data Protection Regulation on Medical Research*. *19*, 1–6. https://doi.org/10.2196/jmir.7108

Mcafee, A., & Brynjolfsson, E. (2012). Spotlight on Big Data Big Data: The Management Revolution. *Harvard Business Review*, (October), 1–9. Retrieved from http://tarjomefa.com/wp-content/uploads/2017/04/6539-English-TarjomeFa-1.pdf

Merriam-Webster. (2020). Retrieved January 12, 2020, from https://www.merriam-webster.com/dictionary/private

Miranda, J., Mäkitalo, N., Garcia-Alonso, J., Berrocal, J., Mikkonen, T., Canal, C., & Murillo, J. M. (2015). From the Internet of Things to the Internet of People. *IEEE Internet Computing*, *19*(2), 40–47. https://doi.org/10.1109/MIC.2015.24

Mowery, D. C., & Simcoe, T. (2002). Is the Internet a US invention? - An economic and technological history of computer networking. *Research Policy*, *31*(8–9), 1369–1387. https://doi.org/10.1016/S0048-7333(02)00069-0

Multistakeholder Expert Group (EU). (2019). *REPORT – CONTRIBUTION FROM THE MULTISTAKEHOLDER EXPERT GROUP TO THE STOCKTAKING EXERCISE OF JUNE 2019 ON ONE YEAR OF GDPR APPLICATION*. (June), 1–22.

Murumaa-mengel, M., Pruulmann-vengerfeld, P., & Laas-Mikko, K. (2014). *The right to privacy as a human right and everyday technologies*.

O'Brien, D., & Torres, A. M. (2012). Social Networking and Online Privacy: Facebook Users' Perceptions. *An Introduction to Social Media Marketing*, 149–165. https://doi.org/10.4324/9780203727836-13

OECD. (1980). *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.

Plangger, K., & Montecchi, M. (2020). Thinking Beyond Privacy Calculus: Investigating Reactions to Customer Surveillance. *Journal of Interactive Marketing*, *50*, 32–44. https://doi.org/10.1016/j.intmar.2019.10.004

Prosser, W. (1960). Privacy. *California Law Review*, *48*, 383–423. https://doi.org/10.4324/9781315246024-13

Qin, Y., Sheng, Q. Z., Falkner, N. J. G., Dustdar, S., Wang, H., & Vasilakos, A. V. (2016). When things matter: A survey on data-centric internet of things. *Journal of Network and Computer Applications*, *64*, 137–153. https://doi.org/10.1016/j.jnca.2015.12.016

Robertson, L., & Muirhead, B. (2020). *Digital Privacy in the Mainstream of Education*. *18*(7), 118–125.

Rosenblum, D. (2007). What Anyone Can Know. *IEEE Security & Privacy*, *5*(3), 40–49.

Roza, R. H. (2018). Revolução Informacional e os Avanços Tecnológicos da Informática e das Telecomunicações. *Pesquisa Brasileira Em Ciência Da Informação e*

Biblioteconomia, *13*(1), 3–11. https://doi.org/10.22478/ufpb.1981-0695.2018v13n1.39230

Shastri, S., Wasserman, M., & Chidambaram, V. (2019). The seven sins of personal-data processing systems under GDPR. *11th USENIX Workshop on Hot Topics in Cloud Computing, HotCloud 2019, Co-Located with USENIX ATC 2019*, (i).

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, *90*(4), 1087–1155. https://doi.org/10.2307/3481326

Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and Challenges for Realising the Internet of Things The meaning of things lies not in the things themselves, but in our attitude towards them. Antoine de Saint-Exupéry. In *Cluster of european research project on Internet of Things*. https://doi.org/10.2759/26127

Susan B. Barnes. (2006). A privacy paradox: Social networking in the United States. *Peer-Reviewed Journal on the Internet*. Retrieved from https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312

Taddicken, M. (2014). The "Privacy Paradox" in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure1. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. https://doi.org/10.1111/jcc4.12052

Tan, L. (2010). Future internet: The Internet of Things. *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, *5*, V5-376-V5-380. https://doi.org/10.1109/ICACTE.2010.5579543

Tang, Q. (2020). Privacy-Preserving Contact Tracing: Current solutions and open questions. *ArXiv*, 1–18.

UN. (n.d.). https://www.un.org/en/universal-declaration-human-rights/. Retrieved from https://www.un.org/en/universal-declaration-human-rights/

UN. (1948). *Universal declaration of human rights*.

UTAIL / JurisAPP. (2019). *Avaliação do Impacto Legislativo do Regulamento Geral de Proteção de Dados (RGPD)*. *679*.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *IV*, 193–220.

Westbrook, G., & Angus, A. (2020). Top 10 Global Consumer Trends in 2016. *Euromonitor International*, 51. Retrieved from http://www.tableau.com/sites/default/files/media/top8bigdatatrends2016_final_1.pdf?ref=lp&signin=9e959a4adc3e8bd87ca238066f07d945&1[os]=mac os x

Westin, A. F. (1968). Privacy and Freedom. In *Washington and Lee Law Review* (Vol. 166).

WHO. (2020). Contact tracing in the context of COVID-19. *WHO Guidelines*, *2019*(May, 10), 1–7. Retrieved from https://www.who.int/publications-detail/contact-tracing-in-the-context-of-covid-19

Williams, M., Nurse, J. R. C., & Creese, S. (2016). The perfect storm: The privacy paradox and the Internet-of-things. *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, 644–652. https://doi.org/10.1109/ARES.2016.25

www.statista.com. (2020). Retrieved January 14, 2020, from https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Zaslavsky, A., Perera, C., & Georgakopoulos, D. (2013). *Sensing as a Service and Big Data*. (July). Retrieved from http://arxiv.org/abs/1301.0159

6. ANNEXES

6.1. Questionnaire perceived impact for citizens

Regulamento Geral de Proteção de Dados para os cidadãos

Begin of section: Dados demográficos

Q1.1 Idade:

- ○ 18-25
- ○ 26-35
- ○ 36-45
- ○ 46-55
- ○ 56-65
- ○ Mais de 65

Q1.2 Género:

- ○ Feminino
- ○ Masculino
- ○ Outro _____

Q1.3 Distrito:

▼ Aveiro ... Madeira

Q1.4 Nível de escolaridade:

- ○ Ensino Básico
- ○ Ensino Secundário
- ○ Licenciatura
- ○ Mestrado
- ○ Doutoramento
- ○ Outro _____

Q1.5 Profissão:_____

Q1.6 Setor de atividade:

▼ Agricultura, criação de animais, caça, silvicultura, mineração e extração ... Outras actividades de serviços coletivos, sociais e pessoais, excepto atividades diversas (57)

End of section: Dados demográficos

Begin of section: Utilização da Internet

Q2.1 Com que frequência utiliza a Internet?

- ○ Diariamente (23)
- ○ 2-3 vezes por semana (25)
- ○ Uma vez por semana (24)
- ○ Uma vez por mês (28)
- ○ Nunca (27)

Proceed to: End of section if Q3.1 = Nunca

Q2.2 Para que utiliza a Internet? (Por favor, selecione todas as alternativas aplicáveis)

- ○ Fazer pesquisas
- ○ Consultar o e-mail
- ○ Usar as redes sociais
- ○ Ler notícias
- ○ Fazer compras
- ○ Procurar emprego
- ○ Ouvir música
- ○ Ver filmes/séries
- ○ Jogar online
- ○ Outro _____

End of section: Utilização da Internet

Begin of section: Privacidade

Q3.1 Indique o seu grau de concordância com a seguinte afirmação: "A privacidade é importante para mim".

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Nem concordo nem discordo
- ○ Discordo parcialmente
- ○ Discordo totalmente

End of section: Privacidade

Begin of section: Privacidade

Q4.1 Indique o seu grau de concordância com a seguinte afirmação: "Conheço técnicas para garantir privacidade e a proteção dos meus dados na utilização da Internet."

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Nem concordo nem discordo
- ○ Discordo parcialmente
- ○ Discordo totalmente

Q4.2 Considera que os seus dados são guardados durante a sua utilização da Internet?

- ○ Sim (23)
- ○ Não (24)

Proceed to: Q5.6 if Q5.2 = Não

Q4.3 Por que meios os seus dados são recolhidos? (Por favor, selecione todas as alternativas aplicáveis)

- ○ Imagens (câmaras fotográficas, circuitos internos de televisão, scanners)
- ○ Sons (microfones, escutas de chamadas, gravadores)
- ○ Questionários (dados pessoais, interesses...)
- ○ Cookies
- ○ Hackers e Crackers (acesso não autorizado aos meus dispositivos)
- ○ GPS e outros dispositivos de localização

Q4.4 Que tipo de informações podem ser obtidas através dos dados recolhidos? (Por favor, selecione todas as alternativas aplicáveis)

- ○ Informação sobre hábitos
- ○ Informação sobre a produtividade de um trabalhador
- ○ Informação sobre o tipo de comprador
- ○ Informação sobre visitas a locais através dos dados de geolocalização
- ○ Informação sobre a utilização dos websites / aplicações
- ○ Outro _____

Q4.5 O que podem fazer as empresas com os dados recolhidos e armazenados? (Por favor, selecione todas as alternativas aplicáveis)

- ○ Criar modelos para facilitar a minha utilização na Internet
- ○ Criar perfis dos clientes
- ○ Criar modelos para otimizar as ofertas aos clientes (por exemplo, os prémios dos seguros)
- ○ Enviar ofertas para os clientes
- ○ Vender os dados recolhidos a outras empresas
- ○ Adequar a publicidade que vejo, aquilo que procuro
- ○ Adaptar a publicidade e sugestões a locais próximos de onde me encontro
- ○ Outro _____

Q4.6 Da seguinte lista de empresas, selecione as 3 que considera terem o melhor comportamento relativamente à privacidade e à proteção dos seus dados.

- ○ Amazon
- ○ eBay
- ○ Ali Express
- ○ Google (Google, Youtube, Google Maps)
- ○ Microsoft, LinkedIn
- ○ Facebook, Instagram, Whatsapp
- ○ TikTok
- ○ Apple
- ○ Samsung
- ○ Huawei
- ○ Xiaomi
- ○ Spotify
- ○ Netflix
- ○ HBO
- ○ Booking
- ○ airbnb
- ○ Uber
- ○ Revolut
- ○ Paypal
- ○ Outro _____

Q4.7 Da seguinte lista de empresas, selecione as 3 que considera terem o pior comportamento relativamente à privacidade e à proteção dos seus dados.

- ○ Amazon
- ○ eBay
- ○ Ali Express
- ○ Google (Google, Youtube, Google Maps)
- ○ Microsoft, LinkedIn
- ○ Facebook, Instagram, Whatsapp
- ○ TikTok
- ○ Apple
- ○ Samsung
- ○ Huawei
- ○ Xiaomi
- ○ Spotify
- ○ Netflix
- ○ HBO
- ○ Booking
- ○ airbnb
- ○ Uber
- ○ Revolut
- ○ Paypal
- ○ Outro _____

End of section: Privacidade

Begin of section: Privacidade na utilização de smartphones

Q5.1 Durante o seu dia-a-dia, utiliza o telemóvel para aceder à Internet?

- ○ Sempre
- ○ Frequentemente
- ○ Ocasionalmente
- ○ Raramente
- ○ Nunca

Q5.2 Indique o seu grau de concordância com a seguinte afirmação: "Preocupo-me com a minha privacidade durante a utilização do meu smartphone para aceder à Internet."

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Nem concordo nem discordo
- ○ Discordo parcialmente
- ○ Discordo totalmente

Q5.3 Indique o seu grau de concordância com a seguinte afirmação: "Considero que o meu smartphone garante a minha privacidade durante a sua utilização"

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Nem concordo nem discordo
- ○ Discordo parcialmente
- ○ Discordo totalmente

Q5.4 Indique o seu grau de concordância com a seguinte afirmação: "Considero que aceder à Internet através do meu smartphone é mais seguro do que através de um computador".

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Nem concordo nem discordo
- ○ Discordo parcialmente
- ○ Discordo totalmente

Q5.5 Qual é a marca do seu smartphone?_____

Q5.6 Indique o seu grau de concordância com a seguinte afirmação: "Procuro bloquear a recolha de dados de aplicações instaladas no meu smartphone".

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Nem concordo nem discordo
- ○ Discordo parcialmente
- ○ Discordo totalmente

End of section: Privacidade na utilização de smartphones

Begin of section: Regulamento Geral de Proteção de Dados

Q6.1 Já ouviu falar do Regulamento Geral de Proteção de Dados?

- ○ Sim
- ○ Não

Proceed to: Q7.3 Se Q7.1 = Não

Q6.2 Por que meios obteve mais informação sobre o Regulamento Geral de Proteção de Dados?

- ○ Televisão
- ○ Internet
- ○ Jornais
- ○ Amigos
- ○ Instituição de Ensino
- ○ Trabalho
- ○ Outro _____

Q6.3 O Regulamento Geral de Proteção de Dados, RGPD, é um quadro jurídico europeu focado na proteção dos dados pessoais, quer na recolha como na gestão dos mesmos.
Indique a opção correta: Dados pessoais são:

- ○ Apenas o nome, e-mail, data de nascimento e número de identificação fiscal
- ○ Todos os anteriores e os detalhes bancários
- ○ Todos os anteriores, informação médica e imagens da minha cara (dados biométricos)
- ○ Tudo aquilo que eu considero pessoal

Q6.4 Quando utiliza um website, costuma ler a sua Política de Privacidade?

- ○ Nunca
- ○ Raramente
- ○ Ocasionalmente
- ○ Frequentemente
- ○ Sempre

End of section: Regulamento Geral de Proteção de Dados

Begin of section: Regulamento Geral de Proteção de Dados: Cookies

Q7.1 Cookies (identificadores únicos do seu dispositivo) são ficheiros de texto armazenados pelos browsers nos computadores e asseguram informação sobre as visitas dos utilizadores aos websites e as suas preferências pessoais.

Q7.2 Com que frequência aceita essa política de cookies?

- ○ Sempre
- ○ A maioria das vezes
- ○ Cerca de metade das vezes
- ○ Algumas vezes
- ○ Nunca

Q7.3 Pensando apenas nas situações em que aceita / toma conhecimento da política de cookies, qual é o principal para essa decisão?

- ○ É a única forma de aceder ao website
- ○ Percebo de que se trata e concordo com a política apresentada
- ○ Não percebo de que se trata mas não me parece relevante

End of section: Regulamento Geral de Proteção de Dados: Cookies

---

Begin of section: Regulamento Geral de Proteção de Dados: Processamento de informação pessoal

Q8.1 “Os titulares dos dados têm direito a opor-se ao uso de profiling, ou seja, qualquer forma automatizada de processamento de informação pessoal, com o objetivo de avaliar e tipificar indivíduos com base nos seus dados pessoais.” Regulamento Geral de Proteção de Dados

Q8.2 Tem conhecimento do conceito de 'Profiling' ou 'Processamento de informação pessoal de forma automatizada'?

- ○ Sim
- ○ Não

Q8.3 Considera que a sua atividade na Internet contribui para o desenvolvimento de profiling?

- ○ Sim
- ○ Não

Q8.4 Selecione, entre as duas opções seguintes, que alternativa vai mais ao encontro das suas preferências:

- ○ Não permitir acesso aos seus dados pessoais e receber anúncios menos interessantes
- ○ Dar acesso aos meus dados pessoais para receber anúncios interessantes e que vão de encontro ao que procuro

End of section: Regulamento Geral de Proteção de Dados: Processamento de informação pessoal

---

Begin of section: Regulamento Geral de Proteção de Dados

Q9.1 Indique o seu grau de concordância com a seguinte afirmação: "Os meus dados ficaram mais protegidos depois da implementação do Regulamento Geral de Proteção de Dados".

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Nem concordo nem discordo
- ○ Discordo parcialmente
- ○ Discordo totalmente

Q9.2 Indique o seu grau de concordância com a seguinte afirmação: "O Regulamento Geral de Proteção de Dados tornou a forma como empresas gerem os meus dados pessoais mais transparente."

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Nem concordo nem discordo
- ○ Discordo parcialmente
- ○ Discordo totalmente

Q9.3 O Regulamento Geral de Proteção de Dados confere a possibilidade de solicitar a qualquer empresa que detenha os seus dados (selecione todas as alternativas aplicáveis):

- ○ Informação e acesso
- ○ Retificação e apagamento
- ○ Limitação de tratamento
- ○ Portabilidade
- ○ Oposição a decisões individuais automatizadas (incluindo a criação de perfis)

End of section: Regulamento Geral de Proteção de Dados

Begin of section: Procedure

Q10.1 Alguma vez exerceu (ou tem conhecimento de alguém que o tenha feito) algum dos direitos que o Regulamento Geral de Proteção de Dados lhe confere?

- ○ Sim
- ○ Não

Proceed to: End of Questionnaire if Q11.1 = Não

Q10.2 Por que meio exerceu esse direito?

- ○ E-mail
- ○ Carta registada
- ○ Pessoalmente (em loja, por exemplo)
- ○ Chamada
- ○ Outro _____

Q10.3 Indique o seu grau de concordância com a seguinte afirmação: "O processo foi simples e transparente."

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Nem concordo nem discordo
- ○ Discordo parcialmente
- ○ Discordo totalmente

Q10.4 Quanto tempo, em média, demorou a receber uma resposta? _____

Q10.5 Tendo em conta esse processo, como classifica:

	Muito insatisfatório	Insatisfatório	Adequado	Satisfatório	Muito satisfatório
Procedimento	○	○	○	○	○
Tempo	○	○	○	○	○
Facilidade	○	○	○	○	○
Transparência	○	○	○	○	○
Clareza	○	○	○	○	○
Resultado	○	○	○	○	○

End of section: Procedure

End of questionnaire

6.2. Questionnaire StayAway Covid

Begin of section: Medidas de controlo da pandemia

Q1.1
"(...) a identificação de casos, isolamento, testagem, cuidados, rastreio de contactos e quarentena são atividades críticas para reduzir a transmissão e controlar a epidemia". Organização Mundial de Saúde, Maio 2020.

Q1.2 Considero que o conjunto de medidas adoptadas em Portugal para controlo da pandemia foi:

- ○ Extremamente adequado
- ○ Parcialmente adequado
- ○ Nem adequado nem inadequado
- ○ Parcialmente inadequado
- ○ Extremamente inadequado

Q1.3 Considero que o peso no meu dia-a-dia do conjunto de medidas adoptadas em Portugal para controlo da pandemia foi:

- ○ Extremamente excessivo
- ○ Parcialmente excessivo
- ○ Nem excessivo nem insuficiente
- ○ Parcialmente insuficiente
- ○ Extremamente insuficiente

End of section: Medidas de controlo da pandemia

Begin of section: StayAway Covid

Q2.1 A aplicação StayAway Covid, cuja utilização é voluntária, através de códigos aleatórios difundidos por Bluetooth, informa os utilizadores da existência de um contacto dos últimos 14 dias que, entretanto, teste positivo.

Q2.2 Uma das formas de rastreio de contactos preparada é uma aplicação móvel. Utilizaria essa aplicação voluntariamente?

- ○ Certamente que sim
- ○ Provavelmente sim
- ○ Talvez
- ○ Provavelmente não
- ○ Certamente que não

Proceed to: Q3.4 if Uma das formas de rastreio de contactos preparada é uma aplicação móvel. Utilizaria essa aplicaçã... = Certamente que sim

Proceed to: Q3.4 if Uma das formas de rastreio de contactos preparada é uma aplicação móvel. Utilizaria essa aplicaçã... = Provavelmente sim

Proceed to: Q3.3 if Uma das formas de rastreio de contactos preparada é uma aplicação móvel. Utilizaria essa aplicaçã... = Talvez

Proceed to: Q3.3 if Uma das formas de rastreio de contactos preparada é uma aplicação móvel.

Utilizaria essa aplicaçã... = Provavelmente não

Proceed to: Q3.3 if Uma das formas de rastreio de contactos preparada é uma aplicação móvel. Utilizaria essa aplicaçã... = Certamente que não

Q2.3 Porquê?

- ○ Não sei como funciona a aplicação.
- ○ Tenho receio que dados sobre a minha localização sejam partilhados.
- ○ Não sei como vão ser tratados os dados recolhidos.
- ○ Tenho receio que outras pessoas saibam que estou infetado/a.
- ○ Prefiro aguardar que a aplicação seja mais testada.
- ○ Outro _____

Q2.4 Escolha, entre as opções seguintes, que alternativa vai ao encontro das suas preferências:

- ○ Utlizaria a aplicação móvel para que, caso eu fosse diagnosticado com COVID-19, os meus contactos pudessem ser notificados, sem que a minha identidade fosse partilhada.
- ○ Utilizaria a aplicação móvel para, caso algum dos meus contactos fosse diagnosticado com COVID-19, eu pudesse ser notificado.
- ○ Opção 1 e 2.
- ○ Não utilizaria a aplicação.

Q2.5 Caso obtivesse um teste positivo para COVID-19, marcar-se-ia como infetado na aplicação de rastreio de contactos?

- ○ Certamente que sim
- ○ Provavelmente sim
- ○ Talvez
- ○ Provavelmente não
- ○ Certamente que não

Q2.6 Porquê? _____

Q2.7 Indique o seu grau de concordância com a seguinte afirmação: "A utilização de uma aplicação de rastreio de contactos coloca em risco a minha privacidade e / ou a proteção dos meus dados pessoais".

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Nem concordo nem discordo
- ○ Discordo parcialmente
- ○ Discordo totalmente

Q2.8 Escolha, entre as opções seguintes, que alternativa vai ao encontro das suas preferências:

- ○ A saúde pública sobrepõe-se aos meus receios relativamente à privacidade e proteção de dados
- ○ A privacidade e proteção de dados pessoais são tão importantes como a saúde pública
- ○ A privacidade e proteção de dados pessoais sobrepõem-se a esta forma de zelar pela saúde pública

End of section: StayAway Covid

Begin of section: Utilização

Q3.1 Utiliza a aplicação StayAwayCovid?

- ○ Sim
- ○ Não
- ○ Instalei previamente mas entretanto desinstalei.

Proceed to: End of section if Utiliza a aplicação StayAwayCovid? = Sim

Proceed to: Q13 if Utiliza a aplicação StayAwayCovid? = Não

Proceed to: Q13 if Utiliza a aplicação StayAwayCovid? = Instalei previamente mas entretanto desinstalei.

Q3.2 Porquê? _____

End of section: Utilização

Begin of section: Dados demográficos

Q4.1 Idade

- ○ Menos de 18
- ○ 18 - 24
- ○ 25 - 34
- ○ 35 - 44
- ○ 45 - 54
- ○ 55 - 64
- ○ 65 - 74
- ○ 75 - 84
- ○ 85 ou mais

Q4.2 Nível de Ensino

- ○ Ensino Básico
- ○ Ensino Secundário
- ○ Licenciatura
- ○ Mestrado
- ○ Doutoramento

Q4.3 Género

- ○ Feminino
- ○ Masculino
- ○ Outro

Q4.4 Distrito onde reside

▼ Aveiro ... Madeira

Q4.5 Qual das seguintes opções se aproxima mais do setor onde trabalha?

▼ Agricultura ... Finanças, economia ou gestão

Q4.6 Profissão _____

End of section: Dados demográficos

End of questionnaire