

iscte

INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Viver sem segredos - A privacidade dos dados pessoais na era dos Smartphones

Bruno Tomé De Oliveira

Mestrado em Gestão de Sistemas de Informação

Orientadora:

Doutora Inês Messias, Professora auxiliar convidada,
ISCTE-IUL

Maio, 2020



TECNOLOGIAS
E ARQUITETURA

Departamento de Tecnologias e Arquitetura ISTA

Viver sem segredos - A privacidade dos dados pessoais na era dos Smartphones

Bruno Tomé De Oliveira

Mestrado em Gestão de Sistemas de Informação

Orientadora:

Doutora Inês Messias, Professora auxiliar convidada,
ISCTE-IUL

Maio, 2020

Direitos de cópia ou Copyright
©Copyright: Bruno Tomé de Oliveira.

O Iscte - Instituto Universitário de Lisboa tem o direito, perpétuo e sem limites geográficos, de arquivar e publicitar este trabalho através de exemplares impressos reproduzidos em papel ou de forma digital, ou por qualquer outro meio conhecido ou que venha a ser inventado, de o divulgar através de repositórios científicos e de admitir a sua cópia e distribuição com objetivos educacionais ou de investigação, não comerciais, desde que seja dado crédito ao autor e editor.

“Ultimately, saying that you don’t care about privacy because you have nothing to hide is no different from saying you don’t care about freedom of speech because you have nothing to say.”

(Snowden, 2019)

Agradecimentos

Apesar de este trabalho parecer bastante solitário, todo trabalho deste género não é possível de realizar unicamente pelo seu autor principal. Ocorrem vários desafios durante uma dissertação onde encontrar a melhor opção e escolhas adequadas se torna um trabalho coletivo. Não me é possível mencionar todas as pessoas que participaram diretamente ou indiretamente no meu estudo. No entanto, cabe nestas linhas o agradecimento aos que mais me ajudaram neste percurso:

Em primeiro lugar, à minha orientadora, Professora Doutora Inês Messias, pela sua dedicação e pelo seu apoio que tornaram este trabalho possível e uma excelente experiência de aprendizagem. Fico grato pela amizade criada ao longo deste percurso.

Ao Professor Doutor Bráulio Alturas e Professor Doutor Abílio Oliveira, por terem encaminhado o meu percurso na preparação e no início da minha dissertação, fornecendo-me comentários e sugestões de grande utilidade.

Aos excelentes Professores do ISCTE que me disponibilizaram dez minutos da aula para poder apresentar o tema da minha dissertação aos alunos do primeiro ano da escola ISTA do ISCTE, de forma a que estes pudessem perceber de que se trata o meu estudo e de forma a conseguir despertar-lhes a vontade/disponibilidade para participar no mesmo.

Um agradecimento também aos incríveis estudantes do ISCTE que participaram no meu estudo. Tendo em conta que houve uma participação superior a trezentos alunos, podemos dizer que nesse aspeto a sua ajuda foi preciosa.

Não pode faltar um enorme agradecimento à minha família e aos meus amigos, em especial à minha mãe Ana Paula. Sem o apoio, carinho e esforço incondicional que recebi, não me teria sido possível enfrentar e levar este desafio até ao fim. Obrigado por me transmitir o sentimento de orgulho.

Por fim, não conseguiria acabar os agradecimentos sem mencionar a minha querida avó Norbina Moreira, uma pessoa fundamental, que sempre me deu inspiração para ser uma pessoa melhor, mais humilde, conquistar os meus objetivos e que me mostrou que dar e ajudar nos levam ao caminho certo para encontrar felicidade na vida. Fez sempre questão de estar a par da minha dissertação. Infelizmente, na reta final do meu trabalho,

Bruno Oliveira - Viver sem segredos - A privacidade dos dados pessoais na era dos Smartphones

sofreu um trágico acidente. Não estará presente para o ver finalizado, mas sempre me disse que eu ia conseguir. Sinto orgulho por ter um bocadinho desta pessoa em tudo o que sou hoje.

Um sincero “Obrigado”.

Bruno Oliveira

Resumo

Atualmente, verifica-se que os *Smartphones* têm enfrentado um grande crescimento a nível mundial na vida das pessoas. As inúmeras vantagens destes dispositivos para os seus utilizadores têm sido cada vez mais evidentes. Estes aparelhos vivem da partilha de informação: os utilizadores não só recebem a informação pretendida, como também a podem partilhar. No entanto, em muitas instâncias, o utilizador acaba por partilhar dados privados sem se aperceber, sem ter conhecimento, e muitas vezes sem o seu consentimento - dados estes que são recolhidos pelas empresas de telecomunicações e, pior ainda, vendidos a terceiros.

Assim, esta partilha de dados descontrolada através do *Smartphone* pode implicar riscos e até mesmo ameaçar o direito de privacidade dos seus utilizadores, incluindo também aqueles com quem se troca dados através do *Smartphone*.

Este estudo propõe-se a compreender até que ponto os estudantes universitários sabem que a sua privacidade está a ser posta em causa através da utilização de *Smartphones*. O objetivo central do estudo é perceber se, por um lado, este grupo de utilizadores se preocupa com a sua privacidade digital enquanto usa *Smartphones* ou se, por outro lado, lhes é indiferente o facto de terceiros conseguirem ter acesso aos seus dados privados sem o seu consentimento.

Foram utilizadas duas técnicas para a recolha de dados: a) a entrevista com a observação dos alunos, b) o inquérito. Produziu-se um guião para as entrevistas com o objetivo de registar e observar comportamentos com o *Smartphone*. Por fim, elaborou-se um questionário com o intuito de recolher dados sobre a atividade, interação e opinião na utilização do telemóvel. A construção de ambas as ferramentas para a recolha de dados foram elaboradas com recurso ao modelo *TUM*, para que fosse possível, com uma adaptação deste modelo, medir a aceitação da tecnologia dos *Smartphones* juntamente com os riscos de privacidade de dados privados.

Com os resultados obtidos, concluiu-se que os estudantes que participaram neste estudo, de um modo geral, não estão dispostos a abdicar da utilidade que o *Smartphone* lhes dá, mesmo que tal signifique que terceiros tenham acesso aos seus dados privados registados pelos aparelhos. Por outras palavras, pode-se dizer que estão dispostos a ter uma vida transparente perante as organizações que lhes disponibilizam os serviços através do *Smartphone* e perante terceiros que acedem a esses mesmos dados privados.

Palavras-Chave: Tecnologias móveis, Dispositivos móveis, Cibersegurança, Privacidade de Informação, Alunos universitários, Comportamento com Smartphones, Privacidade com Smartphones, Privacidade Digital

Abstract

Smartphones have shown tremendous worldwide growth in the lives of people around the world. The numerous advantages of these devices for their users have been increasingly evident. These devices live by sharing information, where users not only receive the desired information, but can also share information. However, in many instances, the user shares private data without realizing it, without being aware of it and even without their consent, data that is collected by the telecommunications companies and even worse sold to unknown third parties.

This uncontrolled data sharing through the Smartphone can mean risks and even threaten the privacy right to its users, including also the users with whom data is exchanged via the Smartphone.

This study aims to understand the extent to which university students know that their privacy is being called into question through the use of smartphones. A central objective of the study is to understand whether this group of users is concerned with their digital privacy while using Smartphones or whether, on the other hand, they are indifferent to the fact that third parties gain access to their private data without their consent.

Two techniques were used for data collection: a) the interview with the students' observation, b) the survey. A guide was developed for the interviews in order to record and observe behaviors with the Smartphone. The prepared questionnaire was used to collect data on the activity, interaction and opinion in their respective use of the Smartphone. The construction of both tools for data collection were elaborated using the TUM model, so that it was possible, with an adaptation of this model, to measure the acceptance of Smartphones technology together with the privacy risks of private data.

With the results obtained, it was concluded that the students in this study are in no way willing to give up the utility that the Smartphone gives them, even if it means that third parties have access to their private data registered by the Smartphones. In other words, it can be said that they are willing to have a transparent life before the organizations that make services available to them through their Smartphone and third parties that access these same private data.

Keywords: Mobile Technologies, Mobile Devices, Cybersecurity, Information Privacy, College Students, Behavior with Smartphones, Smartphones Privacy, Digital Privacy

Zusammenfassung

Smartphones haben weltweit ein enormes Wachstum im Leben der Menschen erlebt. Die zahlreichen Vorteile dieser Geräte für ihre Benutzer werden immer deutlicher. Diese Geräte leben vom Austausch an Informationen, wobei Benutzer nicht nur die gewünschten Informationen erhalten, sondern auch Informationen gemeinsam nutzen können. Es scheint jedoch, dass der Benutzer in vielen Fällen private Daten teilt, ohne dies zu bemerken, ohne es zu erkennen und sogar ohne seine Zustimmung mit den Telekommunikationsunternehmen und noch schlimmer zu unbekanntem Anbieter.

Dieser unkontrollierte Datenaustausch über das Smartphone kann Risiken bergen und sogar die Datenschutzrechte seiner Benutzer gefährden. Dies gilt auch für die Benutzer, mit denen er Daten über das Smartphone austauscht.

In dieser Studie soll untersucht werden, inwieweit die ISCTE Studenten im ersten Studienjahr wissen, dass ihre Privatsphäre durch die Verwendung ihres Smartphones beeinträchtigt wird. Ein zentrales Ziel der Studie ist es zu verstehen, ob diese Gruppe von Nutzern Bedenken hinsichtlich ihrer digitalen Privatsphäre hat, wenn sie mit Smartphones in Kontakt tritt, oder ob es ihnen gleichgültig ist, dass Dritte Anbieter auch ohne ihre Zustimmung auf ihre privaten Daten zugreifen können.

Für die Datenerfassung wurden zwei Techniken verwendet: a) das Interview mit der Beobachtung der Schüler, b) die Umfrage. Für die Interviews wurde ein Leitfaden entwickelt, um Verhaltensweisen mit dem Smartphone aufzuzeichnen und zu beobachten. Der vorbereitete Fragebogen wurde verwendet, um Daten zur Aktivität, Interaktion und Meinung bei der jeweiligen Nutzung des Smartphones zu sammeln. Die Konstruktion beider Tools zur Datenerfassung wurde anhand des TUM-Modells ausgearbeitet, so dass mit einer Anpassung dieses Modells die Akzeptanz der Smartphones-Technologie zusammen mit den Datenschutzrisiken privater Daten gemessen werden konnte.

Mit den erzielten Ergebnissen wurde der Schluss gezogen, dass die Studierenden in dieser Studie in keiner Weise bereit sind, all die Nützlichkeit, die ein Smartphone ihnen zur Verfügung stellt aufzugeben, auch wenn dies bedeutet, dass Dritte Zugriff auf ihre auf den Smartphones registrierten privaten Daten haben. Mit anderen Worten, kann gesagt werden, dass sie bereit sind, ein transparentes Leben zu führen, wo die Organisationen, die ihnen Dienste über ihr Smartphone zur Verfügung stellen und ihre Daten bearbeiten und unbekannte Dritte, die auf dieselben privaten Daten zugreifen.

Stichworte: Mobiltechnologien, Mobilgeräte, Cybersicherheit, Datenschutz, Studenten, Verhalten mit Smartphones, Datenschutz mit Smartphones, Digitaler Datenschutz

Índice

Agradecimentos	i
Resumo	iii
Abstract	v
Zusammenfassung	vi
Índice	viii
Índice de Tabelas	xi
Índice de Figuras	xiv
Índice de Gráficos	xv
Lista de Abreviaturas e Siglas	xvii
Capítulo 1 – Introdução	1
1.1. Enquadramento do tema.....	1
1.2. Motivação e relevância do tema	3
1.3. Questões e objetivos de investigação.....	4
1.4. Abordagem metodológica de investigação	6
1.5. Quadro teórico	7
1.6. As etapas do modelo TUM.....	8
1.7. Modelo de aceitação Tecnológica (<i>TAM</i>)	10
1.8. Teoria da Dissonância Cognitiva (TDC).....	11
1.9. Teoria do Nível de Adaptação.....	12
1.10. Estrutura e organização da dissertação.....	12
Capítulo 2 – Revisão da Literatura	14
2.1. Tecnologia Móvel.....	14
2.1.1. <i>Smartphone</i>	14
2.1.2. Aplicações móveis	19
2.2. Cibersegurança	25
2.2.1. Definição de Segurança.....	25
2.2.2. Definição da Privacidade	25
2.2.3. Definição da Privacidade Digital.....	25
2.2.4. Problemas de segurança com dados móveis.....	26
2.2.5. Riscos na utilização das aplicações no <i>Smartphone</i>	27

2.2.6.	Segurança com aplicações móveis.....	28
2.2.7.	Definição da confiança.....	29
Capítulo 3 – Metodologia.....		29
3.1.	Desenho de investigação	29
3.2.	Questões e objetivos de investigação.....	30
3.3.	Amostra	31
3.4.	Guião do procedimento da entrevista	31
3.5.	Técnica de Análise de Dados Quantitativos.....	31
3.6.	Análise quantitativa	35
3.7.	Ferramenta de análise quantitativa <i>SPSS</i>	35
3.8.	Resultados	35
Capítulo 4 – Análise e discussão dos resultados.....		37
4.1.	Recolha de dados	37
4.2.	Fase Quantitativa	40
4.2.1.	Entrevista.....	40
4.2.2.	Conclusões das entrevistas	41
4.2.3.	Questionário – Análise exploratória de dados (AED)	44
4.2.4.	Resultados dos questionários aplicados aos estudantes	47
4.2.5.	Análise e criação dos perfis dos estudantes.....	49
4.2.6.	Análise dos resultados relativamente à Teoria do Nível de Adaptação	58
4.2.7.	Análise dos resultados relativamente à Teoria da Dissonância Cognitiva	62
4.2.8.	Análise dos resultados relativamente à utilização do <i>Smartphone</i>	66
4.2.9.	Análise dos resultados relativamente à facilidade de uso percebida (FUP)	68
4.2.10.	Análise dos resultados relativamente à utilidade percebida (UP)	70
4.2.11.	Análise dos resultados relativamente à intenção comportamental (IC)	72
4.2.12.	Análise dos resultados relativamente ao uso real (UR)	74
4.2.13.	Análise dos resultados relativamente à confiança/segurança relacionada com a tecnologia	76
Capítulo 5 – Conclusões e recomendações		78
5.1.	Principais conclusões	78
5.2.	Contributos para a comunidade científica e empresarial	81
5.2.1.	Implicações ao nível académico	81
5.2.2.	Implicações ao nível empresarial.....	82
5.3.	Limitações e dificuldades do estudo	84
5.4.	Recomendações para investigações futuras	85

Bibliografia.....	86
Anexos e Apêndices.....	93
Anexo A – Exemplos de fuga de dados privados	94
Apêndice A – Gráficos da análise de dados	99
Apêndice B – Tabelas SPSS por pergunta de investigação.....	124
Apêndice C – Conclusões por objetivo de investigação	170
4.2.14. Conclusões por objetivo de investigação	170
4.2.15. Determinar o nível de confiança desta população com as organizações; 170	
4.2.16. Determinar se a população em estudo se sente segura relativamente à sua privacidade pessoal ao usar o <i>Smartphone</i> e as suas aplicações;	173
4.2.17. Determinar o nível de satisfação do tratamento dos dados privados da população pelas organizações;.....	176
4.2.18. Determinar o comportamento com o <i>Smartphone</i> ligado à internet, GPS, câmara, microfone;.....	179
4.2.19. Determinar se a população estudada sabe que tipo de informações está a disponibilizar aos vários tipos de organizações;.....	182
4.2.20. Determinar se a população em estudo aceita que as organizações tenham acesso a todos os dados privados introduzidos no <i>Smartphone</i> ;	185
4.2.21. Determinar se o <i>Smartphone</i> traz vantagens no dia-a-dia para o utilizador; 188	
4.2.22. Determinar a quantidade de utilização do <i>Smartphone</i> ;	190
4.2.23. Determinar se o utilizador é <i>digitally savvy</i> ;.....	192
4.2.24. Determinar o tipo de informações que os utilizadores estão a fornecer às organizações que disponibilizam os serviços através dos <i>Smartphones</i> ;	194
4.2.25. Determinar se a população estudada sabe que tipo de informações está a disponibilizar a terceiros, ao usar o seu telemóvel;.....	197
4.2.26. Compreender e identificar se é preciso tomar medidas futuras, de forma a proteger a privacidade digital de cada utilizador, para garantir uma utilização dos <i>Smartphones</i> que deixe os utilizadores sem medo de expor a sua privacidade;...	200
4.2.27. Perceber que utilização as pessoas fazem dos seus dispositivos móveis; 202	
4.2.28. Determinar se a população aceita ter uma vida digital transparente no futuro; 206	
Apêndice E – Guião da Entrevista.....	211
Apêndice F – Métodos de análise descritiva	221
Apêndice G – Guião do questionário	223

Índice de Tabelas

Tabela 1 – Estudantes por Geração e Sexo	48
Tabela 2 – Frequência de Alunos por Curso e Sexo.....	48
Tabela 3 – Frequência de Alunos por Curso e Geração.....	48
Tabela 4 – Teste Qui-quadrado e V de Crámer por sexo dos estudantes.....	125
Tabela 5 – Razão de chance (Odds Ratio) por Sexo dos estudantes	125
Tabela 6 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	126
Tabela 7 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	127
Tabela 8 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes	128
Tabela 9 - Razão de chance (Odds Ratio) por Sexo dos estudantes.....	128
Tabela 10 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	129
Tabela 11 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	130
Tabela 12 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes	131
Tabela 13 - Razão de chance (Odds Ratio) por Sexo dos estudantes.....	131
Tabela 14 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	132
Tabela 15 – Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	133
Tabela 16 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes	134
Tabela 17 - Razão de chance (Odds Ratio) por Sexo dos estudantes.....	134
Tabela 18 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	134
Tabela 19 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	135
Tabela 20 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes	136
Tabela 21 - Razão de chance (Odds Ratio) por Sexo dos estudantes.....	136
Tabela 22 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	137
Tabela 23 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	138
Tabela 24 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes	139
Tabela 25 - Razão de chance (Odds Ratio) por Sexo dos estudantes.....	140
Tabela 26 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	141
Tabela 27 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	142
Tabela 28 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes	143
Tabela 29 - Razão de chance (Odds Ratio) por Sexo dos estudantes.....	144

Tabela 30 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	145
Tabela 31 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	146
Tabela 32 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes	147
Tabela 33 – Razão de chance (Odds Ratio) por Sexo dos estudantes	147
Tabela 34 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	148
Tabela 35 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	148
Tabela 36 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes	149
Tabela 37 - Razão de chance (Odds Ratio) por Sexo dos estudantes	150
Tabela 38 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	150
Tabela 39 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	151
Tabela 40 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes	153
Tabela 41 - Razão de chance (Odds Ratio) por Sexo dos estudantes	153
Tabela 42 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	153
Tabela 43 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	154
Tabela 44 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes	156
Tabela 45 - Razão de chance (Odds Ratio) por Sexo dos estudantes	156
Tabela 46 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	157
Tabela 47 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	158
Tabela 48 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes	159
Tabela 49 - Razão de chance (Odds Ratio) por Sexo dos estudantes	159
Tabela 50 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	160
Tabela 51 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	160
Tabela 52 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes	162
Tabela 53 - Razão de chance (Odds Ratio) por Sexo dos estudantes	162
Tabela 54 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	164
Tabela 55 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	166
Tabela 56 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes	167
Tabela 57 - Razão de chance (Odds Ratio) por Sexo dos estudantes	167

Tabela 58 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes	168
Tabela 59 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes	169

Índice de Figuras

Figura 1 - Modelo de Uso de Tecnologia TUM.....	7
Figura 2 – Períodos Modelo de Uso de Tecnologia TUM.....	8
Figura 3 - Teoria da Ação Racional (TRA).....	10
Figura 4- Modelo de aceitação da tecnologia (TAM).....	11
Figura 5 - Teoria da Dissonância Cognitiva (TDC)	12
Figura 6 - Representação visual de dispositivo de replicação de voz.....	15
Figura 7 - Representação visual de Telefone comum.....	15
Figura 8 - Representação visual do Telemóvel	15
Figura 9 – Representação visual do Smartphone.....	16
Figura 10 – Vendas de Apple Iphones a nível mundial de 2007 até 2018 (em milhões) 17	
Figura 11 – As diferenças entre telefone, telemóvel e Smartphone	18
Figura 12 – Fórmula modelo da aceitação	34
Figura 13 – Smartphone habits and personal feeling.....	43
Figura 14 – Hábitos de utilização com Smartphones.....	43
Figura 15 - Medição da concordância do observador para dados categóricos.....	47
Figura 16 - Formula modelo da aceitação.....	209
Figura 17 – Equação	221
Figura 18 – Equação Qui-quadrado de independência	221
Figura 19 – Equação Correlação de V Crámer.....	222
Figura 20 – Equação Odds Ratio (Razão de chances)	222

Índice de Gráficos

Gráfico 1 – Dados do Género.....	49
Gráfico 2 – Intervalos de anos de nascimento de amostra completa.....	49
Gráfico 3 - Intervalos de anos de nascimento de amostra relevante para o estudo	50
Gráfico 4 – Inquiridos por curso.....	51
Gráfico 5 – Utilização da internet com Smartphone.....	99
Gráfico 6 – Anos com Smartphone pessoal	99
Gráfico 7 – Como inquiridos se ligam à internet.....	100
Gráfico 8 – Aplicações usadas no Smartphone	100
Gráfico 9 – A frequência online na aplicação favorita por dia.....	100
Gráfico 10 – Hábito de ler instruções ou aprender por tentativa de erro	101
Gráfico 11 – Informações incluídas na conta do Smartphone pelos estudantes.....	101
Gráfico 12 – Conhecimento dos estudantes sobre terceiros acederem aos seus dados registados pelo Smartphone.....	102
Gráfico 13 – Aceitação dos termos de aceitação com implicação dos dados de posicionamento do Smartphone.....	102
Gráfico 14 – Nível de afeto do Smartphone nos estudos dos estudantes.....	102
Gráfico 15 – Escala da perceção dos riscos de aplicações de comunicação antes da aquisição do Smartphone	103
Gráfico 16 - Escala sobre a confiança da partilha de informação na utilização das aplicações antes da aquisição do Smartphone	103
Gráfico 17 - Escala sobre a consideração dos riscos de privacidade na utilização do Smartphone antes da sua aquisição.....	104
Gráfico 18 - Escala sobre a consideração dos riscos de privacidade na utilização da câmara do Smartphone.....	104
Gráfico 19 - Escala sobre a consideração se seria necessário instalar uma aplicação para proteger a sua privacidade.....	105
Gráfico 20 – Preocupação com a privacidade na utilização do Smartphone	105
Gráfico 21 – Estudantes voltariam a comprar um Smartphone se pudessem voltar atrás	106
Gráfico 22 – Expetativas das funcionalidades do Smartphone com a realidade depois da utilização	106
Gráfico 23 – Certeza sobre a utilização do Smartphone	106
Gráfico 24 – Confiança no smartphone pessoal	107
Gráfico 25 – Confortável ao usar o Smartphone	107
Gráfico 26 – Utilizei bem o Smartphone	108
Gráfico 27 – Parar de utilizar smartphone conhecendo os riscos de segurança	108
Gráfico 28 – Utilização do Smartphone para uso académico	109
Gráfico 29 - Regularidade média de utilização	109
Gráfico 30 – Média de tempo por dia de utilização do Smartphone	109
Gráfico 31 – Quantidade de anos em que possui um Smartphone	110
Gráfico 32 – Média de horas de utilização semanal com Smartphone	110
Gráfico 33 – Escala de dificuldade percebida ao aprender a utilizar o Smartphone	111
<i>Gráfico 34 – Escala de nível de esforço mental requerido na utilização do Smartphone</i>	<i>111</i>
Gráfico 35 – Facilidade percebida para comunicar com os seus contactos através do Smartphone.....	112
Gráfico 36 – Flexibilidade de ferramentas do Smartphone para poder utilizar	112

Gráfico 37 - Escala da consideração da facilidade percebida na partilha de fotos, vídeos e estados no Smartphone.....	112
Gráfico 38 – Escala da consideração percebida da flexibilidade na interação com o Smartphone.....	113
Gráfico 39 – Escala de consideração da utilidade percebida na comunicação da rede de contactos pessoais	113
Gráfico 40 - Escala de consideração da utilidade percebida na comunicação da rede de contactos universitários	114
Gráfico 41 - Escala de consideração da utilidade percebida na partilha de fotos, videos e ficheiros através do Smartphone.....	114
Gráfico 42 – Ferramentas de Smartphone como aumento de rapidez em trabalho	114
Gráfico 43 – Aumento da eficiência no trabalho diário com uso do Smartphone.....	115
Gráfico 44 – Escala de afeto sentido pelo Smartphone nos estudos.....	115
Gráfico 45 – Escala sobre a consideração se Smartphone iria ser útil para os estudos, previamente a possuir um.....	116
Gráfico 46 – Utilizar o Smartphone sempre que possível.....	116
Gráfico 47 – Intenções de aumentar o uso das ferramentas dos Smartphone	116
Gráfico 48 – Desejo de ter novas ferramentas no Smartphone	117
Gráfico 49 – Necessidade de tapar a câmara do Smartphone	117
Gráfico 50 – Necessidade de desligar o GPS sempre não utiliza.....	117
Gráfico 51 – Necessidade de desligar o Smartphone quando não se está a utilizar por questões de segurança	118
Gráfico 52 – Intenções de aquisição de aplicativo para proteção de invasão por terceiros	118
Gráfico 53 – Desejo de botão que permite desligar o microfone do Smartphone.....	119
Gráfico 54 – Aplicações de uso frequente no Smartphone	119
Gráfico 55 – Frequência do uso de ferramentas do Smartphone.....	120
Gráfico 56 – Habitualmente usa o Smartphone para partilhar dados/fotografias.....	120
Gráfico 57 – Uso do Smartphone para monitorizar a atividade física/desportiva.....	120
Gráfico 58 – Uso do GPS para atividades físicas	121
Gráfico 59 – Divulgação de informações pessoais pelo Smartphone.....	121
Gráfico 60 – Segurança na partilha de fotos/ficheiros/informações pessoais com Smartphone.....	122
Gráfico 61 – Escala sobre segurança com smartphone na comunicação com contactos ou empresas	122
Gráfico 62 – Escala sobre segurança com smartphone para jogar as mais diversas aplicações	122
Gráfico 63 – Segurança ao utilizar Smartphone em conversas privadas ou dados sensíveis	123

Lista de Abreviaturas e Siglas

3G – *Third Generation of wireless mobile telecommunications technology* (Terceira geração de tecnologia de telecomunicações móveis sem fio)

4G – *Fourth Generation of broadband cellular network* (Quarta geração de rede móvel de banda larga)

5G – *Fifth Generation of broadband cellular network* (Quinta geração de rede móvel de banda larga)

AED - Análise exploratória de Dados

ALT – *Adaptacion Level Theory* (Teoria do nível de adaptação)

DS – Dados sociodemográficos

FUP – Facilidade de Uso Percebida

GPS – *Global Positioning System* (Sistema de Posicionamento Global)

GSM – *Global System for Mobile communications* (Sistema Global para Comunicações Móveis)

GUI – *Graphical User Interface* (Interface gráfica do utilizador)

iOS – *Operation System for iPhones* (Sistema operativo de iPhones)

ISCTE-IUL – Instituto Superior de Ciências do Trabalho e da Empresa – Instituto Universitário de Lisboa

ISTA – Escola de Tecnologias e Arquitetura

LTS – *Location-based tracking system* (Sistema de rastreamento baseado em localização)

PT – Perfil tecnológico

RGPD – Regulamento Geral de Proteção de Dados

SMS – *Short Message Service* (Serviço de Mensagens Curto)

SPSS – *Statistical Package for the Social Sciences* (Programa Estatístico de pacotes para as Ciências Sociais)

TAM – *Theory acceptance model* (Modelo de aceitação tecnológica)

TCD – Teoria da dissonância cognitiva

TOS – *Terms of service* (Termos de serviço)

TRA – Teoria da Ação Racional

TUM – *Technology Usage Model* (Modelo de uso da tecnologia)

URL – *Uniform Resource Locator* (Localizador uniforme de recurso)

WEB – Abv. De World Wide Web (Rede mundial de internet para dispositivos computacionais)

Wi-Fi – *Family of wireless network technologies* (Família de tecnologias de rede sem fio)

Capítulo 1 – Introdução

1.1. Enquadramento do tema

A sociedade digital em que vivemos hoje em dia caracteriza-se pela crescente utilização de dispositivos móveis, que permitem aos utilizadores manter-se permanentemente conectados. Esta realidade espelha-se quer nas nossas vidas profissionais, quer pessoais, tendo até provocado alterações na forma como comunicamos - procuramos informação e produzimos conhecimento (Messias, 2017).

Contudo, ainda que os *Smartphones* nos proporcionem todas estas facilidades de comunicação, trouxeram também alguns aspetos menos positivos, como, por exemplo, a dependência que temos dos mesmos no nosso dia a dia, e algumas questões de privacidade que surgem, muitas vezes, pela necessidade de uso, razão pela qual assistimos, há bem pouco tempo, à alteração da legislação RGPD (Regulamento Geral de Proteção de dados) (Anshari & Alas, 2015).

Esta investigação surge, então, neste contexto de uma crescente utilização de *Smartphones* e das suas respetivas aplicações, procurando determinar o comportamento de utilização de dispositivos ligados à internet relativamente ao uso que fazem das ferramentas base, i.e., *GPS*, câmara, microfone, calendário, e-mail, contactos, mensagens e páginas web.

No relatório publicado em 2020 da ANACOM sobre o tráfego de banda larga móvel, verificou-se que o aumento em 2019 foi de 36,8%, estando associado a um crescimento de 44% aos acessos através de telemóveis.

No ano 2017, em Portugal, foram registados 6,6 milhões de utilizadores efetivos de serviços típicos da banda larga móvel, como vídeo telefonia, transmissão de dados em banda larga, televisão móvel e outros. Notou-se um crescimento de 0,4% face ao trimestre anterior e mais 15,8% em relação ao 1.º trimestre de 2016. Tal pode ser explicado devido ao aumento de utilizadores de Internet no telemóvel, que são mais 19,3% face ao 1.º trimestre de 2016 (ANACOM, 2017). Também no relatório publicado em 2020 da ANACOM sobre o tráfego de banda larga móvel, verificou-se que o aumento em 2019 foi de 36,8%, estando associado a um crescimento de 44% aos acessos através de telemóveis (ANACOM, 2020).

Ademais, “*A report from International Data Corporation has shown that a total of 344.3 million smartphones have been shipped around the world only in the first quarter of 2017 (1Q17), achieving a 3.4% increase over the last year (IDC, 2017).*” (Meng, Wang, Wong, Wen, & Xiang, 2018).

A utilização e o consumo de aplicações móveis estão em crescimento junto com os *Smartphones*. Este mercado que continua em ascensão pode representar uma oportunidade para as empresas (Zhaw, 2014).

O conjunto de oportunidades e vantagens que o *Smartphone* oferece aos seus utilizadores pode ser muito grande. A adoção destes dispositivos é tão elevada que, em muitos mercados, quase todas as pessoas tem um *Smartphone*. Estes podem ser facilmente transportados pelo utilizador para qualquer lado, pois a sua portabilidade, em combinação com o seu formato compacto, permite facilmente aos utilizadores ter o *Smartphone* consigo a toda a hora. As relações sociais dos utilizadores podem, graças a este aparelho, ser cuidadas a longa distância e em qualquer lugar, significando que a conectividade destas relações fica constantemente disponível através de telefonemas, mensagens, entre outros.

O facto de estes aparelhos disponibilizarem uma capacidade de armazenamento de dados relativamente grande - em alguns casos mil *Gigabytes* - evidencia que é possível os utilizadores armazenarem uma grande quantidade de dados privados no *Smartphone*. Alguns exemplos podem ser: o histórico de comunicações com outros utilizadores, os contactos na sua agenda, os históricos do navegador de internet e até dados sobre os locais que o utilizador frequenta.

Tendo em conta todos estes fatores mencionados acima, percebe-se o interesse em investigar até que nível os utilizadores da nossa população em estudo se preocupam com estes riscos e ameaças ligadas à utilização do *Smartphone* e se a indústria de *Smartphones* tem de alterar os seus comportamentos correspondentes à recolha de dados dos utilizadores. A verificação de um número elevado de desagrado dos utilizadores com o tratamento dos seus dados privados pode significar uma desvantagem competitiva da respetiva empresa perante uma empresa que não permita aos seus *Smartphones* a recolha de dados privados e mantenha o mínimo de informação possível sobre o utilizador armazenada, no *Smartphone*.

1.2. Motivação e relevância do tema

A investigação surge pela crescente utilização de *Smartphones*, pelas suas respetivas aplicações assim como pela determinação do comportamento com dispositivos ligados à internet relativamente à utilização de *GPS*, câmara, microfone, calendário, e-mail, contactos, mensagens e páginas web.

Nesta linha de raciocínio, escolha deste tema deve-se à constatação dos problemas acima mencionados relativamente à utilização das tecnologias, das telecomunicações e à problemática que surge relativamente à proteção de dados pessoais dos utilizadores de *Smartphones*. No seguimento do meu interesse pela referida problemática, surge este estudo, que pretende perceber se os estudantes do primeiro ano do ISCTE da escola ISTA, que representam em grande parte as gerações *i Generation* e *Digital Natives*, partilham o mesmo interesse em proteger os seus dados pessoais e se sentem necessidade de ter alguns cuidados específicos com o seu *Smartphone*.

Sendo este problema de dados pessoais relativamente recente para muitos utilizadores de *Smartphones*, é importante que se desenvolvam estudos sobre os comportamentos dos utilizadores e de como estes interagem com os dispositivos.

A tecnologia está a evoluir a cada dia que passa e permite, cada vez mais, o desenvolvimento de métodos eficazes e rápidos de registar os dados pessoais de cada utilizador. Isto dá lugar a que as empresas registem dados dos utilizadores sem que estes se apercebam e, com isto, criar perfis de cada utilizador que podem ser utilizados para diversos fins, como o *marketing*.

O objetivo é identificar as tendências futuras do comportamento dos utilizadores e perceber se demonstram alguns cuidados no uso dos *Smartphones* em relação à disponibilização de dados pessoais. Com base nesta amostra representativa da população, será possível perceber e identificar se é necessário tomar medidas futuras de forma a ajudar as pessoas a protegerem a sua privacidade digital.

Neste sentido, “A presença pessoal pode ser facilmente captada, registada e disseminada por uma miríade de dispositivos tecnológicos, sem autorização ou consentimento, expondo cada indivíduo à completa transparência da sua esfera de

personalidade para um contingente indecifrável de pessoas, sem barreiras temporais e espaciais” (Ghisi & Pezzella, 2014).

1.3. Questões e objetivos de investigação

A correta definição dos objetivos é essencial, de forma a poder explicar com clareza a questão de investigação e os respetivos problemas envolventes, permitindo, assim, a possibilidade de obter respostas de forma eficaz e eficiente (McDaniel & Gates, 2004).

É objetivo deste estudo determinar a posição que a população tem relativamente ao uso e tratamento de dados pessoais que são registados pelos *Smartphones* e determinar quais as medidas necessárias a tomar, para no futuro garantir uma utilização dos mesmos que deixe os utilizadores sem medo de expor a sua privacidade.

É necessário saber qual o ponto de vista da população em estudo sobre este assunto, por forma a compreender e identificar a eventualidade de tomar medidas futuras, com o intuito de proteger a privacidade digital de cada utilizador.

Assim sendo, o propósito deste estudo é entender o tipo de informações que os utilizadores estão, possivelmente, a fornecer às organizações que disponibilizam os serviços através dos *Smartphones* e também compreender se gravam dados privados diretamente no aparelho. Posto isto, será possível perceber se a população estudada sabe que tipo de informações está a disponibilizar aos vários tipos de organizações, ao usar o seu telemóvel. Com estes dados, poder-se-ão encontrar indicadores que demonstrem se a população em causa está pronta a ter uma vida transparente perante estas organizações.

O conhecimento gerado também permitirá perceber que utilização as pessoas fazem dos seus dispositivos móveis.

Por fim, com este estudo, pretende-se, igualmente, obter indicadores, de forma a constatar se a população aceita uma vida digital transparente no futuro. Note-se, no entanto, que as questões que envolvem previsões futuras serão feitas sobre um cenário ideal, pelo que estas podem não se verificar de uma forma exata relativamente aos tempos que se seguem.

Para ficarmos a perceber o que esta população aceita e até que nível está disposta a abdicar da sua privacidade digital, pretende-se estudar um conjunto de indivíduos através de inquéritos para:

- a) Determinar o nível de confiança desta população com as organizações;
- b) Determinar se a população em estudo se sente segura relativamente à sua privacidade pessoal ao usar o *Smartphone* e as suas aplicações;
- c) Determinar o nível de satisfação do tratamento dos dados privados da população pelas organizações;
- d) Determinar o comportamento com o *Smartphone* ligado à internet, *GPS*, câmara, microfone;
- e) Determinar se a população estudada sabe que tipo de informações está a disponibilizar aos vários tipos de organizações;
- f) Determinar se a população em estudo aceita que as organizações tenham acesso a todos os dados privados introduzidos no *Smartphone*;
- g) Determinar se o *Smartphone* traz vantagens no dia-a-dia para o utilizador.
- h) Determinar a quantidade de utilização *Smartphone*;
- i) Determinar se o utilizador é *digitally savvy*;
- 1) Determinar o tipo de informações que os utilizadores estão a fornecer às organizações que disponibilizam os serviços através dos *Smartphones*;
- 2) Determinar se a população estudada sabe que tipo de informações está a disponibilizar a terceiros ao usar o seu telemóvel;
- 3) Compreender e identificar se é preciso tomar medidas futuras de forma a proteger a privacidade digital de cada utilizador, para garantir uma utilização dos *Smartphones* que deixe os utilizadores sem medo de expor a sua privacidade;
- 4) Perceber que utilização as pessoas fazem dos seus dispositivos móveis;
- 5) Determinar se a população aceita ter uma vida digital transparente no futuro.

Sendo os objetivos gerais do estudo listados de a) a i) e os objetivos de 1) a 5) são os objetivos específicos de privacidade.

Com os resultados futuros, espera-se entender se a tendência do aumento do uso dos *Smartphones* vai continuar com as leis de proteção de dados atuais.

Este estudo enquadra-se no âmbito do Mestrado de Sistemas de Informação, do ISCTE, desenvolvido no contexto científico dos *Smartphones* nas áreas de tecnologias móveis, dispositivos móveis, cibersegurança e privacidade de informação.

Propõe-se a compreender, com este estudo, até que ponto os estudantes universitários do primeiro ano de licenciatura da escola ISTA do ISCTE sabem que a sua privacidade

está a ser posta em causa através dos *Smartphones* e se tomam medidas para impedir que o *Smartphone* possa recolher dados em situações da sua vida privada. Pretende-se saber como se sentem com esta ameaça digital, que permite que as empresas que desenvolvem aplicações móveis possam gravar e analisar dados pessoais, de maneira a registar a vida privada do utilizador de uma forma sistemática, na qual, em seguida, é possível construir um perfil do utilizador através da análise de biga data (Anshari & Alas, 2015).

Tentar-se-á perceber se têm comportamentos como desligar o *Smartphone*, os dados móveis ou até mesmo deixar o *Smartphone* em algum lugar, para evitar que recolham os seus dados pessoais através do mesmo, havendo um maior foco em entender se este grupo de utilizadores se preocupa com a sua privacidade digital ou se lhes é indiferente o facto de terceiros, possivelmente, terem acesso aos seus dados privados, até mesmo sem o seu consentimento.

Com estes resultados, será possível indagar as tendências futuras sobre o que as duas gerações *i Generation* (>2000) e *Digital Natives* (1991-2000) aceitam ou não em relação à recolha de dados privados através do *Smartphone*, com e sem o seu consentimento, de forma a identificar se os desenvolvedores dos sistemas operativos dos *Smartphones* necessitam ou não de alterar a forma como agem com os seus utilizadores. Por fim, pretende-se denotar a possível necessidade de se adaptar a lei, de forma a proteger mais os dados pessoais dos indivíduos com o uso do *Smartphone*.

1.4. Abordagem metodológica de investigação

Adotar-se-á uma estratégia de investigação quantitativa, na qual se irão, pois, recolher dados quantitativos, através da técnica de questionário, com respostas fechadas, o que implica seguir um guião que será exposto aos inquiridos. Os questionários serão feitos a alunos do primeiro ano da escola ISTA do ISCTE, com o objetivo de analisar o sexo, a geração (*i Generation* e *Digital Natives*), o curso e a segurança na utilização dos telemóveis dos mesmos. De salientar, que uma grande vantagem do questionário com resposta fechada é ser adequado para replicar, permitindo facilmente o seu uso em outros estudos, com outras populações.

O modelo *TUM* aplicado neste estudo foi o que permitiu a elaboração do questionário, com a respetiva revisão de literatura. O questionário está dividido em várias partes. Uma parte é sobre os dados sociodemográficos (DS) e sobre o perfil tecnológico (PT), e outra

é sobre o modelo *TUM* com as suas três componentes principais, a teoria do nível de adaptação (*ALT*), a teoria da dissonância cognitiva (*TDC*) e o modelo de aceitação (*TAM*). São aplicadas escalas do tipo *Likert* entre 1 e 5 no questionário, que são construídas na plataforma *Google Forms*. O *SPSS* serve como ferramenta de análise estatística para a análise de dados desta investigação.

1.5. Quadro teórico

Tecnologia nova e inovadora é usada para desenvolver novos serviços. Neste processo, a aceitação e a adoção da tecnologia são grandes desafios. Quando uma inovação é apresentada ao mercado, uma empresa necessita de compreender os fatores que influenciam a decisão de adoção dos potenciais clientes (Frambach & Schillewaert, 2002).

De facto, um dos principais motores para o sucesso empresarial, geralmente, é a inovação da tecnologia (Cardozo, McLaughlin, Harmon, Reynolds, & Miller, 1993).

Tendo em conta que o estudo irá analisar as preocupações e formas de utilização de *Smartphones*, a metodologia a adotar será o *TUM* “*Technology Usage Model*” apresentado na Fig. 1.

O modelo *TUM* aplica a conjunção de três teorias: o Modelo de Aceitação de Tecnologia (*TAM*), a Teoria da Dissonância Cognitiva (*TDC*) e a Teoria do Nível de Adaptação (*ALT*).

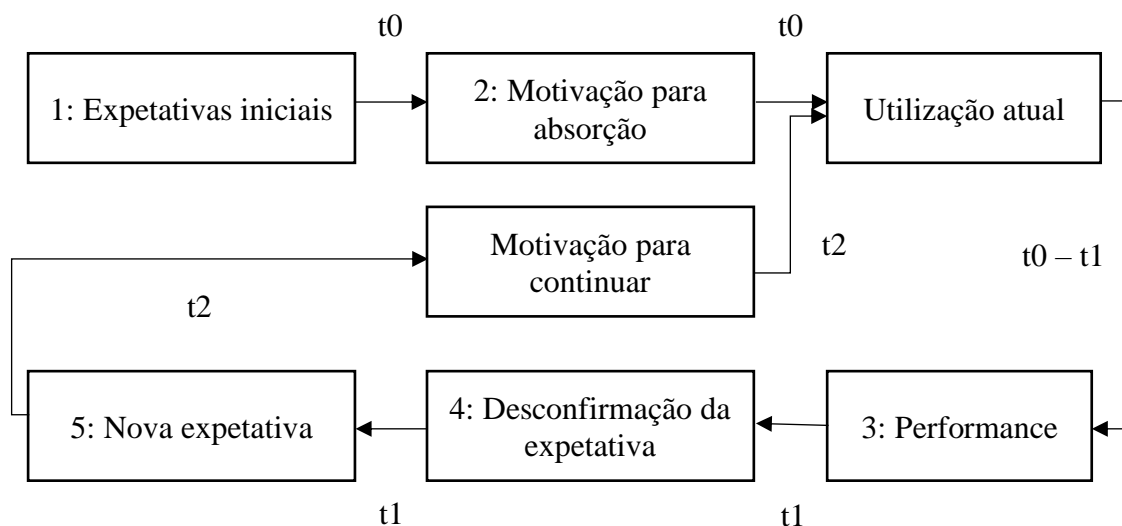


Figura 1 - Modelo de Uso de Tecnologia TUM

Fonte: (Pinpathomrat, 2015)

O modelo *TUM* explica o uso da tecnologia em duas partes, no qual a primeira explica o uso da tecnologia no período de tempo (t_0 a t_1) e a segunda explica o uso da tecnologia no segundo período de tempo (t_1 a t_2). O tempo t_0 representa o ponto de tempo de pré-utilização. Os tempos t_1 e t_2 representam o pós-uso um e dois períodos de tempo o que se pode perceber na Fig. 2 (Pinpathomrat, 2015).

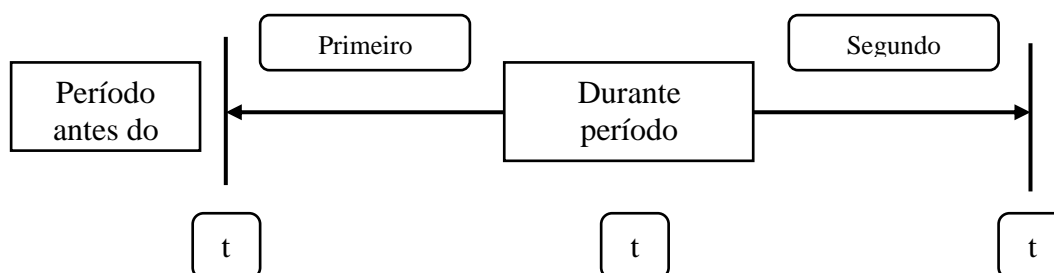


Figura 2 – Períodos Modelo de Uso de Tecnologia TUM

Fonte: (Pinpathomrat, 2015)

1.6. As etapas do modelo TUM

A primeira etapa é composta pela “expectativa inicial” do utilizador antes da utilização da tecnologia. É nesta etapa que se vai documentar, através de uma entrevista e com um questionário, as expectativas dos utilizadores, de forma a, mais tarde, conseguir compará-las com a quarta etapa, onde se vai verificar a “desconfirmação da expectativa” inicial. A “desconfirmação da expectativa” inicial será obtida depois da “performance” medida na realidade, cuja obtenção será após a observação da utilização real da tecnologia. A quinta etapa será a “nova expectativa”. Esta estará adaptada à realidade e, para isso, será necessário alterar a “expectativa inicial”, comparando-a com a “desconfirmação da expectativa”, de forma a obter uma “nova expectativa” mais coerente com a realidade.

Expectativas iniciais: São as expectativas que o futuro utilizador tem antes de utilizar a tecnologia. Estas expectativas não representam as expectativas reais, visto que o utilizador ainda não utilizou a tecnologia e se encontra no primeiro período antes do uso.

Relativamente ao estudo em questão, será a ideia que o utilizador tem da tecnologia a analisar relativamente à segurança e privacidade.

Motivação para absorção: É o fator que decide se o utilizador realmente adquire a tecnologia. As expectativas iniciais aqui são um fator muito importante para a decisão final.

Relativamente ao estudo em causa, serão as razões que levam os utilizadores a dominar ou saber mais sobre a segurança.

Utilização atual: Quando a motivação para a absorção da tecnologia é suficiente para convencer o utilizador a utilizá-la, este vai, pela primeira vez, usar a tecnologia. É aqui que entramos na segunda etapa. É nesta fase que o utilizador entra no primeiro período de utilização (período de uso).

Tendo em conta o estudo em questão, será nesta fase que vamos verificar o comportamento do utilizador através de uma entrevista.

Performance: A performance é quando o utilizador vai testar a tecnologia e perceber como esta é na vida real. Aqui, o utilizador vai perceber se as expectativas iniciais se aplicam na realidade e como vai utilizar a tecnologia no futuro.

Relativamente ao estudo em causa, será nesta fase que o utilizador vai, durante a entrevista, perceber quais são os riscos que corre ao utilizar o *Smartphone*, e, tomando consciência, aplicar e testar os métodos de segurança na prática.

Desconfirmação das expectativas: A performance vai permitir ao utilizador que, nesta etapa, seja possível comparar as expectativas iniciais com a realidade, de maneira a desconfirmar as expectativas. Com esta desconfirmação das expectativas, o utilizador fica a perceber as vantagens desta tecnologia na vida real.

Tendo em conta o estudo em causa, será nesta fase que o utilizador vai comparar o seu comportamento inicial relativamente à segurança com o comportamento novo desejável.

Nova expectativa: A nova expectativa representa, para o utilizador, o que a tecnologia lhe oferece após a verificação da realidade de utilização.

Relativamente a este estudo, será definido um comportamento novo do utilizador relativamente ao comportamento inicial com a segurança com o *Smartphone*.

Motivação para continuar: Esta etapa permite ao utilizador perceber se esta tecnologia realmente lhe traz vantagens suficientes para continuar a utilizar a mesma. Nesta fase, estamos no segundo período de utilização.

Relativamente ao estudo em causa, será aqui que o utilizador vai decidir se vale a pena continuar com o comportamento definido na nova expectativa, de forma a ter um comportamento mais seguro com o *Smartphone*.

1.7. Modelo de aceitação Tecnológica (TAM)

O modelo de aceitação de tecnologia, *Technology Acceptance Model (TAM)*, é um dos modelos comportamentais mais usados no campo dos sistemas de informação. Este modelo foi projetado para compreender a relação causal entre variáveis externas de aceitação dos utilizadores e o uso real do sistema, através do conhecimento da utilidade e da facilidade de utilização percebida pelo utilizador e, desta forma, pretende entender o comportamento deste utilizador. Este modelo foi construído com base na Teoria da Ação Racional (TRA), por sua vez, desenvolvida por Davis (1989) ilustrada na Fig. 3. A Teoria da Ação Racional afirma, então, que o comportamento dos indivíduos se deve à sua motivação para realizar esse comportamento, ou seja, é uma função compreensiva das expectativas de uma pessoa em relação a um comportamento alvo (R. J. Hill, Fishbein, & Ajzen, 1977).

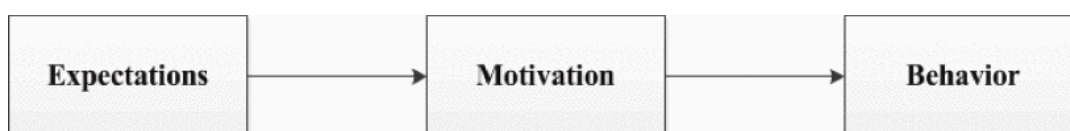


Figura 3 - Teoria da Ação Racional (TRA)

Fonte: (R. J. Hill et al., 1977)

Para melhorar o seu desempenho no trabalho, as pessoas têm que decidir se vão ou não usar uma tecnologia. Mesmo quando uma determinada tecnologia é útil, o utilizador poderá optar pela não utilização da mesma, se o uso for muito complicado, pois, nesse caso, o esforço não compensará esse uso.

A Fig. 4 representa a percepção de que os potenciais utilizadores apenas optam por usar a tecnologia quando acreditam que esta utilização lhes fornecerá resultados positivos, focando-se na percepção da facilidade de uso (*perceived ease of use*) e na percepção da utilidade (*perceived usefulness*). Assim, utiliza-se o modelo TAM para entender o porquê de o utilizador aceitar ou rejeitar a tecnologia de informação. Com este modelo, é também possível, depois, propor uma abordagem para melhorar a aceitação da tecnologia por parte do utilizador, oferecendo um suporte para prever e facilitar a aceitação (Davis, 1989).

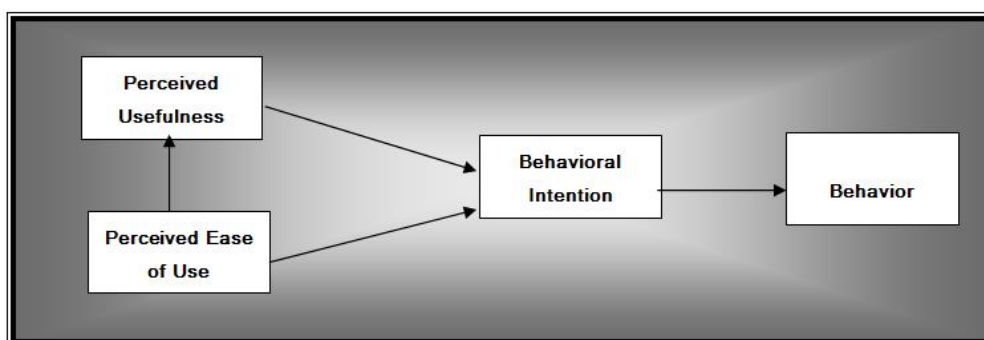


Figura 4- Modelo de aceitação da tecnologia (TAM)

Fonte: (Davis, 1989)

1.8. Teoria da Dissonância Cognitiva (TDC)

A Teoria da Dissonância Cognitiva (TDC) tem por base o pressuposto de que os indivíduos têm a necessidade de manter um nível de consistência entre a sua cognição e a realidade, sugerindo que existe um estado psicológico de dissonância quando a realidade e as estruturas cognitivas, ou seja, as expectativas, são inconsistentes.

A teoria da dissonância cognitiva, proposta pelo psicólogo Leon Festinger (1957) e ilustrada na Fig. 5, tem por objetivo compreender como as pessoas tentam alcançar a consistência interna. Esta teoria diz que as pessoas têm uma necessidade interior de garantir que as suas crenças e comportamentos são consistentes entre eles. As pessoas tentam evitar crenças conflitantes ou inconsistentes que as deixem em desarmonia.

O utilizador da tecnologia de informação pode verificar a dissonância cognitiva no período em que usa as tecnologias, se as expectativas iniciais, as que o levaram à aceitação

da mesma, não se verificarem reais durante a utilização da tecnologia. É comum o utilizador modificar as suas expectativas para ser mais consistente com a realidade (Morvan & O'Connor, 2017).

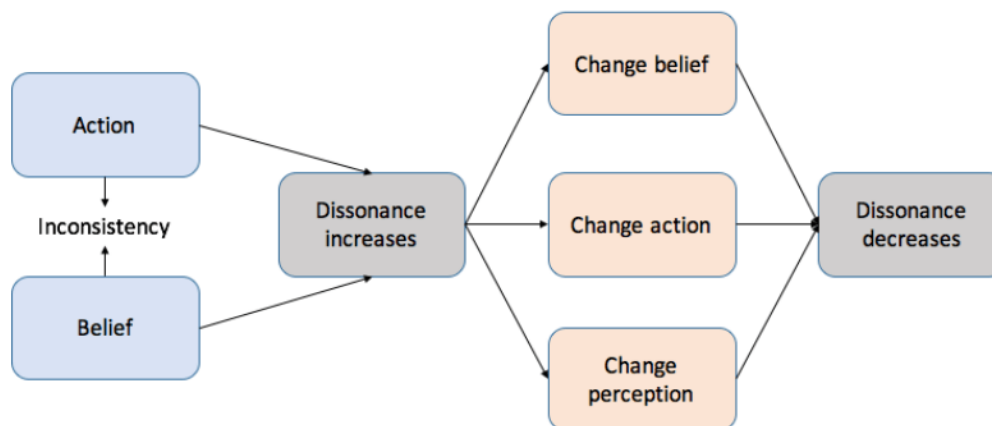


Figura 5 - Teoria da Dissonância Cognitiva (TDC)

Fonte: (Morvan & O'Connor, 2017)

1.9. Teoria do Nível de Adaptação

A Teoria do Nível de Adaptação (ALT - *Adaptation Level Theory*) sugere que as expectativas iniciais dos utilizadores individuais são a base de comparação do seu nível de adaptação. Assim, os utilizadores, através de uma comparação entre o nível de adaptação, a expectativa inicial, e o desempenho real percebido, determinam a desconfirmação do uso da tecnologia. Com a desconfirmação determinada, é possível ajustar a expectativa que existia inicialmente, de forma a obter a nova expectativa, que é mais próxima da realidade (Edwards, 2018).

1.10. Estrutura e organização da dissertação

A presente dissertação é composta por cinco capítulos.

O primeiro capítulo consiste numa secção introdutória, onde é realizada a contextualização do tema e demonstrado o cerne da investigação, seguido da descrição do objetivo e a metodologia escolhida que permitirá obter a resposta ao problema mencionado neste trabalho.

No segundo capítulo, far-se-á a análise do estado de arte, na qual se discutem os estudos desenvolvidos até ao momento, e relevantes para o âmbito desta dissertação. Nesta linha de raciocínio, serão abordados temas como as tecnologias móveis, os dispositivos móveis, a cibersegurança e a privacidade de informação com as aplicações dos *Smartphones* analisadas neste estudo.

No terceiro capítulo, apresentar-se-á a metodologia. Aqui, pretende-se destacar os modelos de aceitação de tecnologia, de maneira a analisar os tipos de comportamento dos utilizadores, para adoção e uso de *Smartphones*, que coloquem em risco a divulgação de dados pessoais e a privacidade. A metodologia *TUM* é a base deste estudo exploratório, que expõe uma abordagem qualitativa, e que permitirá perceber o comportamento dos utilizadores e como estes aceitam esta tecnologia. Uma vez que este estudo pressupõe a observação e registo de comportamento dos utilizadores de *Smartphones*, escolheu-se a entrevista e o questionário como ferramentas de recolha de dados necessários ao estudo.

No quarto capítulo, apresentar-se-á a análise dos dados recolhidos para esta dissertação. Para a análise dos dados quantitativos, de resposta fechada, recolhidos na entrevista e no questionário, escolheu-se a ferramenta *SPSS*. Toda a amostragem do estudo quantitativo, com os gráficos e as tabelas geradas pelo *SPSS*, será aqui apresentada.

No quinto capítulo, mostrar-se-ão um conjunto de conclusões finais, que incluem as limitações deste estudo, as recomendações para a utilização segura dos dados privados com *Smartphones* e também possíveis considerações para trabalhos futuros.

Numa secção final da atual dissertação, é exposta a amostragem completa do estudo qualitativo e todas as citações dos utilizadores inquiridos neste trabalho.

Capítulo 2 – Revisão da Literatura

2.1. Tecnologia Móvel

A tecnologia móvel, é uma categoria ampla, que aborda todo tipo de dispositivos e infraestruturas que permitem ao utilizador comunicar e trocar dados com outros utilizadores, ou também sistemas em todo mundo e a todo o momento (Lim, 2008).

Para que os utilizadores consigam utilizar os dispositivos móveis, de forma a terem a mobilidade que estes possibilitam e conseguirem fazer as suas transações em qualquer lugar, têm de ter acesso a uma rede móvel (Au & Kauffman, 2008).

Em seguida, com o propósito de compreender a evolução dos telefones tradicionais até aos *Smartphones*, serão apresentadas, as três grandes evoluções tecnológicas desses dispositivos, tal como os números de vendas do *Smartphone* mais popular da atualidade. As suas ferramentas e aplicações que vem já de fábrica e que caracterizam este tipo de dispositivo serão, também, evocadas o que permitirá uma melhor compreensão acerca do *Smartphone*. As aplicações focadas neste estudo, que vem por defeito já no aparelho no momento da compra, são: navegador *Web*, *GPS*, calendário, e-mail, agenda de contactos, câmara, microfone e mensagens.

2.1.1. *Smartphone*

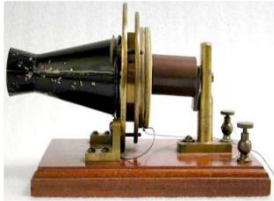
Os *Smartphones* são a última geração de telefones móveis. Estes dispositivos têm várias funções semelhantes às de um computador normal, como o acesso a emails, browser e outros serviços com rede móvel acessível através de ligação por satélite e apresentando uma maior portabilidade e um preço mais acessível, e permitindo todas as funções inerentes a um telefone comum.

Nas palavras de Hill, “*A smartphone is a handheld device, capable of providing wireless voice communications along with support for other applications. Data applications typically include messaging (both text and multimedia), e-mail, audio players, and Web surfing via a Graphical User Interface (GUI)-based browser (versus the more primitive type of handheld devices with text-based browsing).*” (D. Hill, 2018).

Uma vez que este estudo pretende analisar as questões de segurança inerentes à utilização dos *Smartphones*, torna-se interessante traçar uma linha temporal destes aparelhos.

- Telefone comum

Relativamente ao telefone comum, criado pelo emigrante escocês Alexander Graham Bell, foi o primeiro a receber uma patente dos Estados Unidos para um dispositivo que produzia uma replicação claramente inteligível da voz humana, representado na Fig.6. Este avanço tecnológico deu origem para ao telefone comum hoje conhecido, apresentado na Fig. 7.



Telephone-circuit Patented (1881)

Figura 6 - Representação visual de dispositivo de replicação de voz

Fonte: *National Museum of American History*

https://www.si.edu/object/alexander-graham-bell-experimental-telephone:nmah_689864



Fonte: <https://patents.google.com/patent/US244426A/en>

Figura 7 - Representação visual de Telefone comum

Fonte: <https://www.khouryhome.com/alcatel-tel-t50b-black.html>

- Telemóvel

O telemóvel, representado na Fig. 8, que possibilita o envio de mensagens aos seus utilizadores foi o próximo grande avanço na direção aos *Smartphones* de hoje, Hill (2018) fala sobre este fenómeno na seguinte citação abaixo.



“Text messaging was the first, widespread data application for cell phones introduced in the Global System for Mobile communications (GSM) standard in the early 1990s. However, the challenge was using a phone’s keypad to type text messages. Pressing a key several times enabled a single key to represent several letters.” (D. Hill, 2018).

Figura 8 - Representação visual do Telemóvel

Fonte: https://en.wikipedia.org/wiki/Nokia_3410

- *Smartphone*

O *Smartphone*, representado na Fig. 9, foi a evolução seguinte que Hill (2018) menciona no seu trabalho, definindo-a como brilhante. A seguinte citação deste mesmo autor, explica também o fenómeno do ecrã tátil presente nos *Smartphones*.



“The next brilliant stroke of genius in the evolution of smartphone design was the introduction of the touch- screen. This design allows the graphics display to encompass nearly the entire footprint of the smartphone itself, leaving some room on the surface and along the edge, perhaps, for a few buttons, like a power switch and menu selection.” (D. Hill, 2018).

Figura 9 – Representação visual do Smartphone

Fonte: <https://www.apple.com>

O *iPhone* da *Apple* é um exemplo muito popular a nível mundial, o que se pode verificar pelo número de vendas a nível mundial. Vendeu mais de 211 milhões de aparelhos em 2016 como se pode ver na seguinte Fig. 10 (Galloway & Sean Keach, 2016).

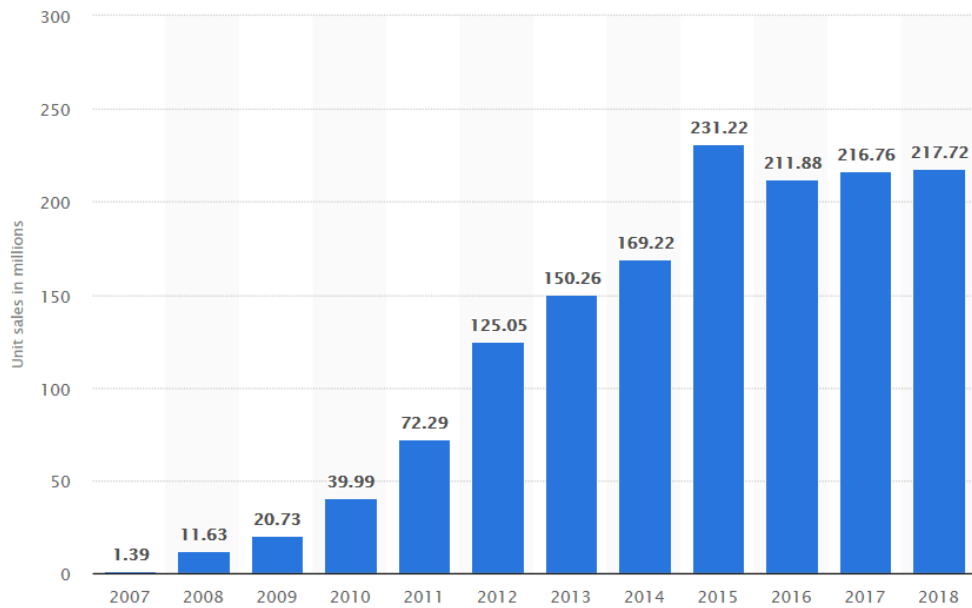


Figura 10 – Vendas de Apple iPhones a nível mundial de 2007 até 2018 (em milhões)

Fonte: <https://www.statista.com/statistics/276306/global-apple-iphone-sales-since-fiscal-year-2007/>

É possível, então, ao verificar a seguinte tabela (Fig. 11), publicada por Yuan (2005), observar a diferença entre as funções suportadas por estes dispositivos. Podemos reparar que existem um conjunto de aplicações que são suportadas por *Smartphones*, mas que não são por um simples telefone comum. Através desta informação, ficam claramente evidentes as principais vantagens de um *Smartphone* comparativamente com um telefone comum, assim como se verifica que um *Smartphone* tem características muito semelhantes às de um computador.

Function	Telephone	Cellphone	Smartphone
Send and receive telephone calls	Yes	Yes	Yes
Receive and store messages	Yes, with answering machine attached or built in	Yes	Yes
Camera	No	Some	Yes
Calendar	No	Some, but limited	Yes
Address Book	Some, but usually only names and telephone numbers	Yes	Yes
Music Player	No	No	Yes
Text Messaging	No	Some	Yes
Internet Access	No	Some	Yes
Email	No	Some	Yes
Voice Dialing	No	Some	Yes
Bluetooth	No	Some	Yes
Video Recording	No	Some	Yes
GPS	No	Some	Yes
Office Programs	No	No	Yes
Keyboard	No	Some	Yes

Figura 11 – As diferenças entre telefone, telemóvel e Smartphone

Fonte: (Yuan, 2005)

É com a constatação destas diferenças entre os referidos dispositivos, que se torna possível perceber como e porquê que os *Smartphones* se tornaram rapidamente tão populares. Entre os principais benefícios inerentes aos *Smartphones*, encontram-se, de facto, os seus múltiplos recursos. Mais especificamente, podemos dizer que:

- Os *Smartphones* são aproximadamente do mesmo tamanho, forma e peso que um telemóvel normal.
- Geralmente, têm uma grande quantidade de memória para que possamos armazenar vários dados, tais como ficheiros de músicas, fotografias, vídeos e informações pessoais.
- Os *Smartphones* podem aceder ao e-mail e à web onde quer que o utilizador esteja, seja por meio de uma conexão 4G móvel ou por meio de uma conexão *Wi-Fi*, se esta estiver disponível.
- Os *Smartphones* têm a capacidade de executar aplicativos conhecidos como 'apps' - programas de computador que são executados no telefone. Os aplicativos podem fornecer uma ampla gama de funções, desde processadores de texto até jogos e

tradutores de idiomas estrangeiros. É como ter um computador totalmente funcional no seu bolso.

- Os *Smartphones* também podem fazer e receber chamadas telefônicas e mensagens de texto.
- Os custos com smartphones variam muito de acordo com o modelo e o provedor da rede. Geralmente, o preço de um *Smartphone* varia entre 50,00 € e 1500,00 €.

2.1.2. Aplicações móveis

Este tipo de software, tão característico dos *Smartphones* e que os tornaram tão populares em todo o mundo, é, no entanto, o meio pelo qual os seus criadores têm acesso a grande parte da informação acerca dos seus utilizadores/clientes, pelo que, neste estudo, se optou por apenas considerar para análise as aplicações base, que vêm por defeito em todos os *Smartphones*, e que os utilizadores não podem mesmo desinstalar.

Deste modo, será importante descrevê-las em detalhe:

a) Navegador *Web*

Um Navegador da *Web* é um aplicativo de software que permite aceder às informações na *World Wide Web*.

Cada página da *Web* é identificada por um *URL* distinto, possibilitando que os navegadores da *Web* os exibam no dispositivo do utilizador.

Um navegador da *Web* não é o mesmo que um mecanismo de pesquisa. Para um utilizador, um mecanismo de pesquisa é apenas um *website*, como uma página de internet (i.e. www.google.com), que armazena dados pesquisáveis sobre outros *websites*. Mas, para se conectar e exibir sites no dispositivo, o utilizador precisa de ter um navegador *Web* (como o *Chrome* da *Google*) instalado, é explicado bem com a seguinte citação: “*The increased use of smartphones has established a trend of web browsing through smartphone browsers. On one hand many of the smartphone web browsers are available and on the other hand many of the websites are customized for mobile browsing.*” (Fazal-e-Amin, 2015).

Sendo este o aplicativo mais comum em qualquer computador para o acesso à Internet, e usado para imensas funcionalidades que interagem com dados sensíveis, tal como o comércio online, é preciso proteger os dados pessoais, de forma a que ninguém possa aceder aos mesmos sem ter essa permissão, a seguinte citação descreve bem as funcionalidades no *Web Browser*: “*The web browser is often a user’s window to the world, providing them an interface to perform a wide range of activity including email correspondence, shopping, social networking, personal finance management, and professional business.*” (Ter Louw, Lim, & Venkatakrishnan, 2008).

b) *GPS* (Sistema de Posicionamento Global)

“*GPS is a satellite microwave technique, i.e., its signals are transmitted on microwave (L-band) carriers through the Earth’s atmosphere. There are other satellite microwave techniques like, e.g., the 1030 French DORIS system, the German PRARE system, and the Russian GLONASS system. GPS is the most advanced, and certainly the most widely used technique in geodesy and geodynamics.*” (Rothacher & Beutler, 1998).

De facto, *GPS* é a sigla para *Global Positioning System*. Em português, significa “Sistema de Posicionamento Global”. É uma tecnologia de localização por satélite. Basta ter um dispositivo móvel para poder utilizar o *GPS*, que é um sistema de navegação por satélite. Este sistema envia informações da posição do utilizador desta tecnologia - por exemplo, de um *Smartphone* -, a qualquer horário e em qualquer condição climática. Os *Smartphones*, hoje em dia, possuem o *GPS* integrado e acessível através dos seus próprios aplicativos.

Foi criado em 1973 pelo militar americano para facilitar os sistemas de navegação. Este sistema consiste em 24 satélites que circulam a Terra duas vezes por dia a, aproximadamente, uma altitude de 20,200 km com uma velocidade de, aproximadamente, 11,500 km/h. Assim, é possível garantir que pelos menos quatro satélites estejam sempre visíveis a qualquer ponto da terra e possam trocar dados de posicionamento entre eles. Com isto, o *GPS* funciona em qualquer ponto da Terra e a qualquer momento.

Este sistema é muito utilizado em automóveis e em combinação de sistema de mapas, de forma a facilitar a descoberta de trajetos mais eficientes entre dois pontos.

O poder de localizar e registrar os movimentos dos indivíduos é uma ferramenta que pode ser um risco para os utilizadores de *Smartphones*. Se terceiros tiverem acesso a este tipo de dados, os utilizadores podem colocar a sua privacidade em risco. Segue uma citação interessante que explica o fenómeno de registrar a localização de objetos. *“Location-based tracking systems (LTSs) use a variety of technologies to record the locations of objects. An LTS can increase the risks to the privacy and security of individuals.”* (Wang & Loui, 2009).

c) Calendário

“Digital calendars have been heavily influenced by the design of the physical calendar and have invariably adopted their grid representation of days in the month.” (Hund, Dowell, & Mueller, 2014).

A aplicação do calendário serve para gerir o tempo, gerir a sua agenda, e pode incluir os lembretes referentes ao que o utilizador agendar, tais como reuniões e aniversários, ajudando, desta forma, a gerir eventos. Se terceiros tiverem acesso a este tipo de informação do utilizador, podem, entre outras coisas, obter dados sensíveis sobre a sua privacidade, como explicado na seguinte citação.

“Mobile systems, the networks they connect to, and the apps they run can all be exploited to steal sensitive information such as documents, calendar appointments, email messages, texts, and attachments.” (Check Point, 2017).

Como já observado no passado, existe a possibilidade de roubarem dados sensíveis das aplicações que se conectam com a internet, tais como todos os que podem ser incluídos na aplicação do calendário, visto que esta permite introduzir muitas informações sobre pessoas, encontros e até mesmo assuntos privados. A seguinte citação mostra um exemplo bom em relação a este tema.

“Facebook, for example, syncs and uploads contacts and calendar details, and even records voice during status updates. Although this behavior is associated with the most aggressive types of malware, Facebook isn’t malicious.” (Check Point, 2017).

Os utilizadores que não interpretam corretamente ou não leem os manuais de utilização das aplicações podem estar a partilhar os seus dados com terceiros sem o saber. A

aplicação do calendário é um alvo que muitas aplicações e entidades tem interesse em aceder, como o *Facebook*, por exemplo.

“(...) data may also be corrupted or modified by natural forces (for example, by random data corruption). For example, a malware program might delete or maliciously modify the contents of the mobile device’s address book or calendar.”(Carey, 2011).

Ora, os estudos de (Carey, 2011) mostram que os dados do calendário podem até mesmo ser alterados ou apagados, se o dispositivo estiver infetado com um programa malicioso. O problema de utilizadores destas ferramentas serem alvo de programas maliciosos é grande e é necessário que os utilizadores tenham mecanismos que os possam proteger nestes casos.

d) E-mail

Um e-mail ou também chamado "correio eletrónico". Semelhante a uma carta, o e-mail é enviado pela Internet para o seu destino. É necessário criar um endereço de e-mail, que é exclusivo para um único utilizador, para receber e-mails. Alguns utilizadores usam aplicativos no seu *Smartphone* e outros usam o navegador *Web* para aceder aos seus e-mails.

O uso dos mesmos tem alguns benefícios importantes, como ser muito rápido, ser seguro, ter um baixo custo, poder anexar documentos no e-mail e poder enviar, de uma só vez, para vários destinatários. A citação seguinte verifica-se que a população geral faz uso do e-mail.

“During the past three decades, e-mail has evolved from an Internet application used only by technology specialists to a common communication tool that is embraced by the general population.” (Huang & Lin, 2014).

Por outro lado, o uso do e-mail não está isento de riscos, pois um terceiro pode chegar a muitos dados privados destes utilizadores, se conseguir ter acesso ou descobrir a nossa palavra passe. Além disto, muitas empresas verificam os emails institucionais dos seus funcionários, na procura de evitar fugas de informação. Isto pode significar riscos de segurança dos dados pessoais dos utilizadores, como referido na seguinte citação.

“The truth is that exposure to hacking of you yahoo messenger or any other kind of email supplier account has become quite a problem to users.” (Kim, Shin, Shin, & Zhang, 2011).

e) Agenda de Contactos

A agenda de contactos no “*Smartphone*” serve para gravar os números de telefone de outros indivíduos. O princípio é o mesmo de uma agenda tradicional, mas esta é eletrónica e tem vários recursos extra. Por exemplo, é possível gravar o nome, data de nascimento, número de telefone, e-mail e até o endereço. Tudo isto pode ficar guardado nos servidores da organização do sistema operativo do *Smartphone*.

A sincronização destes dados ocorre se o utilizador sincronizar os contactos com a conta da *Google*, no caso de usar um *Smartphone Android*. Isto pode ser bastante útil, se perder o *Smartphone*, mas também revela tudo sobre os seus contactos a terceiros.

f) Câmaras no *Smartphone*

As câmaras num *Smartphone* já conseguem substituir uma grande parte das câmaras compactas tradicionais de fotografia. Isto faz com que os utilizadores usem estas câmaras para tirar fotografias e gravar vídeos. Os arquivos das fotografias podem ficar guardados fisicamente no *Smartphone* ou então na *cloud*. Neste caso, ficam guardadas na internet e podendo ser acedidas em qualquer lugar com acesso à mesma, e com qualquer dispositivo no qual tenha acesso à sua conta. As empresas têm tendência a apostar na *Cloud* como falado na seguinte citação.

“There is along-lasting trend within enterprise and private computing to fundamentally embrace the cloud.” (Slawik, Zilci, & Küpper, 2018).

Se terceiros obtiverem controlo sobre a câmara de um *Smartphone*, trata-se de uma infração grave na vida de um utilizador. Este tipo de infração é um risco de privacidade que pode estragar a confiança do utilizador na tecnologia ou, neste caso, no *Smartphone*. Como mencionado na seguinte citação.

“All smart phones have features like camera and touch screen, these features may lead to different types of attacks on smartphones.” (Deshpande & Dharmadhikari, 2016).

g) Microfone do *Smartphone*

O microfone dos “*Smartphones*” serve para gravar a voz dos utilizadores em chamadas, vídeo chamadas, mensagens de voz e em inúmeras outras aplicações, com várias finalidades.

Tal como na câmara, o microfone é algo que pode causar um risco de privacidade grande para um utilizador. Dado que todos os *Smartphones* têm, obrigatoriamente, um microfone, para podermos iniciar e receber as chamadas, isto significa que é possível que um terceiro registre todos os sons provenientes de um utilizador (independentemente de serem do próprio ou do que o rodeia). Algumas aplicações de *Smartphone* são capazes de fazer este tipo de registos, de forma a gravar conversas de utilizadores, tal como a famosa *Siri*, nos sistemas *iOS* da *Apple*. A seguinte citação mostra que existem diferentes formas de atacar um *Smartphone*.

“There are different sources of attacks on Smartphones. These attacks do not only affect the Smartphones, but also influence telecommunication networks since Smartphones are endpoints between internet and telecommunication networks.” (Waheed & Khan, 2010).

h) Aplicação de Mensagens

Um *SMS (Short Message Service)* é um serviço de mensagens curtas. Este é um dos serviços mais usados para a troca de mensagens de textos curtos, que podem ser enviados e recebidos com dispositivos móveis.

Através de um *SMS*, uma mensagem tem um processo de envio e receção muito simples. O utilizador do *Smartphone* só necessita de escrever a mensagem na aplicação de mensagens, no seu aparelho, e inserir o número da pessoa a quem quer enviar. A mensagem será enviada com sucesso. As seguintes citações mostram a importância de existir métodos capazes de classificar o tipo de mensagens.

“SMS (Short Message Service) is one of popular ways of communication between millions of people, where transmission of messages must occur according to communication standard protocols. Therefore, there is a need for text classification algorithms that can be used in classifying the messages either to ham or spam messages.” (Suleiman & Al-Naymat, 2017).

“There are different sources of attacks on Smartphones. These attacks do not only affect the Smartphones, but also influence telecommunication networks since Smartphones are endpoints between internet and telecommunication networks.” (Waheed & Khan, 2010).

2.2. Cibersegurança

2.2.1. Definição de Segurança

O termo segurança vem do latim “*securitas*” e implica minimizar ou eliminar qualquer tipo de risco na vida. Quando se obtém uma qualidade de segurança, podemos dizer que é possível viver sem nenhum tipo de medo. A segurança implica, assim, o estado de estar protegido. Pode-se descrever a segurança como um conjunto de medidas assumidas para se proteger de atos de violência, tais como ataques de espionagem, roubos, sabotagens entre outros (Conceito.de, 2011).

2.2.2. Definição da Privacidade

A Privacidade é o direito à reserva de informações pessoais e da própria vida pessoal. Pode também dizer-se que é “literalmente o direito de ser deixado em paz”. Isto foi o que o jurista norte-americano Louis Brandeis (Warren and Brandeis 1890), juntamente com Samuel Warren, formulou como conceito do direito à privacidade. A vontade de controlar a exposição de informações sobre si mesmo é também uma boa definição da privacidade. A seguinte citação dos autores referidos mostra uma forte representação do direito a estar sozinho.

“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.” (Warren & Brandeis, 1890).

Também se pode dizer que a privacidade ocorre em “*situações confidenciais, sigilosas ou secretas*” (Conceito.de, 2013).

2.2.3. Definição da Privacidade Digital

O conceito da privacidade digital é a possibilidade de qualquer pessoa conseguir controlar a exposição e a disponibilidade de informações sobre ela mesma, sobre um

conhecido ou até mesmo sobre um desconhecido no mundo digital. Temos como exemplo o que acontece nos sites de partilha de informação ou redes sociais online. Com a arquitetura atual da internet, é possível desenvolver novas tecnologias de controlo de informação, de forma a alterar individualmente a forma como cada pessoa vê a privacidade. Vale a pena mencionar o centro nacional de cibersegurança de Portugal, o qual descreve boas práticas para um cidadão ciberseguro (Cibersegurança, 2020).

Com a falta de leis consolidadas em relação à privacidade digital, cada utilizador tem de estar preparado para enfrentar novas situações de invasões da privacidade, no mundo digital, com novas tecnologias.

2.2.4. Problemas de segurança com dados móveis

A empresa *Security Research Labs* dedicou dois investigadores a um estudo com engenharia-inversa. Analisou centenas (1200) de *Smartphones Android*, onde descobriram diversas fraudes relacionadas com as atualizações de versões de segurança dos *Smartphones* (Lell & Nohl, 2018).

Os investigadores Karsten Nohl e Jakob Lell, que se centraram em fazer engenharia-inversa no código do sistema operativo *Android*, detetaram diversos problemas, sobretudo mentiras por parte dos fabricantes. De um modo mais preciso, algumas marcas de *Smartphones* garantem, na informação que disponibilizam aos utilizadores, que os dispositivos têm as atualizações de segurança até uma certa data, mas, na realidade, ignoraram dúzias de *patches* correspondentes a esse período, o que não garante a segurança prometida aos seus utilizadores.

Os modelos mais antigos acabam por ser ignorados e abandonados pelas empresas em relação às atualizações de segurança, de forma a poupar recursos. No entanto, estes mantêm a informação de que foram atualizados na mesma, enganando o utilizador (Lell & Nohl, 2018).

Os *Smartphones* podem aceder à internet ao usar uma rede *Wi-Fi* ou então uma rede móvel, tais como redes 3G, 4G e 5G. Os riscos de sofrer um ataque malicioso no *Smartphone* aumentam quando a conexão com estas redes são contínuas e ocorrem durante longos períodos. Assim “terceiros”, com intenções maliciosas, podem usar

aplicações no *Smartphone* para obter informações do seu alvo (Delac, Silic, & Krolo, 2011).

Efetivamente, *“Since the mobile devices are in effect becoming storage units for personal data, they are an attractive target for breaching user’s privacy.”* (Delac et al., 2011).

As redes *Wi-Fi* representam um papel importante nas casas dos utilizadores e para as empresas que as utilizam, mas, mesmo assim, estas redes de *Wi-Fi* são relativamente fracas no que diz respeito à segurança das mesmas: *“With easily available directional antennas, attackers can be physically located off-site, yet compromise WiFi security protocols such as WEP, WPA, and even to some extent WPA2 through a range of exploits specific to those protocols, or simply by running dictionary and human-factors attacks on users’ poorly-chosen passwords.”* (Xiong & Jamieson, 2013).

2.2.5. Riscos na utilização das aplicações no *Smartphone*

“Smartphones can assist users in a variety of activities, i.e., from social networking to online shopping, but also have become an attractive target for cyber-criminals due to the stored personal data and sensitive information.” (Meng et al., 2018).

Através das aplicações móveis, os utilizadores compartilham dados pessoais, que podem incluir a localização e os hábitos do dia-a-dia. Estes utilizadores estão a oferecer uma forma livre para que terceiros, com potenciais más intenções, sejam capazes de rastrear os passos de possíveis vítimas.

Vários aplicativos dos *Smartphones* coletam a localização dos utilizadores em tempo real, como se pode ler nos termos de utilização (regras de utilização) destes aplicativos. Estes podem até compartilhar estas informações com terceiros, livremente. A seguinte citação explica que as aplicações dos *Smartphones* enviam dados a terceiros.

“The research that we and our colleagues are doing identifies and explores a significant threat that most people miss: More than 70 percent of smartphone apps are reporting personal data to third-party tracking companies like Google Analytics, the Facebook Graph API or Crashlytics.” (Vallina-Rodriguez & Sundaresan, 2017).

É de conhecimento geral que a maioria dos utilizadores não lê os termos de utilização dos aplicativos quando os vai utilizar pela primeira vez e a maioria dos utilizadores que

o faz não fica a perceber totalmente o que isto significa como é mencionado na citação seguinte (Obar & Oeldorf-Hirsch, 2018).

“The front page of their website reads ‘I have read and agree to the Terms’ is the biggest lie on the web. (...) The role of the clickwrap in facilitating policy acceptance is worth emphasizing. Of the 543 individuals surveyed, 74 percent accepted the privacy policy via the quick-join clickwrap option which allowed participants to bypass the policy without even requiring a glimpse. Qualitative responses suggest that 78 percent of individuals often use the quick-join clickwrap option and more than 90 percent use it often or sometimes.” (Obar & Oeldorf-Hirsch, 2018).

Uma vítima destes eventos pode ser a bateria do *Smartphone*. Esta pode descarregar muito mais rápido, visto que estes aplicativos estão constantemente a coletar, analisar e enviar dados.

Por fim, é possível que o *Smartphone* seja infetado com qualquer tipo de vírus, se não usar estes aplicativos com o devido cuidado.

2.2.6. Segurança com aplicações móveis

A falta de proteção binária é um risco de segurança nas aplicações móveis. Na ausência desta proteção, poder-se-á, fazendo engenharia inversa do código do aplicativo, injetar um *malware* no aplicativo pirateado com uma possível ameaça. É uma preocupação crítica na segurança de aplicativos móveis, pois pode resultar num roubo de dados confidenciais, causar danos à marca e à confiança, fraudes, perdas de receita, e outras consequências negativas para a vítima. Para evitar estes riscos, é muito importante que as empresas dos aplicativos móveis usem técnicas de proteção binária nas aplicações.

Com uma percentagem de 98% dos aplicativos móveis analisados no relatório *Arxan's fifth annual State of Application Security Report* (Arxan, 2016), este estudo chegou à conclusão de que a proteção binária era insuficiente. Isto pode ter como consequência a manipulação do código do aplicativo, o sucesso na realização de uma engenharia inversa e o roubo de dados e violações de privacidade. *“Lack of binary protection (98%) – this was the most prevalent vulnerability”* (Arxan, 2016).

2.2.7. Definição da confiança

A confiança é definida como a disposição de um indivíduo a estar exposto a ações de outro indivíduo, na esperança de que este execute uma certa atividade importante para ele - isto, independentemente de ter a capacidade de controlar esse indivíduo. Para o compartilhamento de informação, a confiança cara-a-cara é um critério crítico, o que também é importante na troca de informação online (Shin, 2010); (Dwyer, Roxanne Hiltz, Passerini, & Roxanne, 2007).

A troca de informação online também ocorre no uso de *Smartphones*.

Por isso, na teoria social, a confiança é muito importante. Para a interação social, esta teoria da troca social engloba uma análise de custo-benefício (Leffler & Roloff, 2006); (Dwyer et al., 2007).

Capítulo 3 – Metodologia

3.1. Desenho de investigação

Qualquer pesquisa deve assentar em alicerces e preocupações metodológicas orientadoras, de modo a garantir coerência e consistência no corpo do trabalho. Ou seja, por metodologia entende-se a especificação de todas as etapas, procedimentos e estratégias utilizadas quer para recolha, quer para o tratamento de dados, de forma a dar resposta às questões de investigação.

O primeiro momento deste estudo passou por fazer a recolha de literatura para se proceder à elaboração do enquadramento teórico, sendo, depois, possível enquadrar o estudo no contexto atual e perceber a sua pertinência. Aqui, denotou-se claramente que os humanos usam os novos meios tecnológicos, tais como o *Smartphone*, como meios de comunicação. As gerações mais novas já têm um conceito de comunicação muito ligado aos *Smartphones*, o que tem levado continuamente a uma mudança cultural e das mentalidades no que toca à comunicação humana.

Num segundo momento, e uma vez que este estudo pretende perceber as preocupações que os estudantes do primeiro ano da escola ISTA do ISCTE têm com a utilização do *Smartphone*, optou-se por se utilizar como quadro metodológico o *TUM*, tal como referido no capítulo 1.5. Este modelo *TUM* engloba vários modelos que permitem obter mais dados sobre o utilizador do *Smartphone*, ao contrário de apenas da aplicação do modelo *TAM*. Optou-se por uma investigação de natureza quantitativa, na qual se recolherão dados através de entrevista estruturada, para uma melhor perceção das respostas quanto ao facto de estarem de acordo com o real uso do objeto de estudo. Definiu-se também a amostra e o contexto onde este estudo será implementado. Por outro lado, a escolha dos participantes para as entrevistas e os questionários deveu-se ao facto de serem alunos do primeiro ano e representarem a população mais jovem da faculdade. Dos quatro cursos seleccionados para este estudo, há dois de tecnologia, tais como Engenharia de Telecomunicações e Informática, o que eleva a probabilidade de termos alunos nas entrevistas e nos questionários que já têm algum conhecimento sobre os assuntos abordados neste estudo. Por outro lado, também temos alunos em cursos “menos tecnológicos”, tal como o curso de Arquitetura, no qual esperamos alunos com menos conhecimento sobre os temas abordados nesta dissertação. Assim sendo, será possível

fazer uma comparação e analisar se existem diferenças de comportamento entre estes estudantes de cursos diferentes na utilização e preocupações do *Smartphone*.

Os dados serão recolhidos após a implementação da entrevista e do questionário, sendo, posteriormente, tratados com recurso ao *SPSS*.

Num último momento, será possível elaborar as conclusões e dar resposta às questões de investigação.

Na primeira parte do estudo, realizaram-se entrevistas estruturadas com oito estudantes, de forma a poder observar se têm comportamentos específicos para se protegerem de qualquer possível registo de informação, através do *Smartphone*, em situações do dia-a-dia. Já na segunda parte do estudo, aplicou-se a técnica de questionário, com o qual se recolheram dados sobre o maior número possível da população em estudo, tendo conseguido uma obtenção de 328 participantes, com 317 respostas validas para este estudo.

3.2. Questões e objetivos de investigação

É objetivo deste estudo saber “até que ponto os estudantes universitários do primeiro ano da escola ISTA do ISCTE sabem que a sua privacidade está a ser posta em causa através dos *Smartphones*.”

Para isso, será necessário analisar os seguintes pontos de comportamento ao utilizar o *Smartphone*:

- Perfil de utilização com *Smartphone*;
- Nível de perceção de riscos na utilização do *Smartphone*;
- Facilidade percebida na utilização do *Smartphone*;
- Utilidade percebida na utilização do *Smartphone*;
- Nível de confiança na utilização do *Smartphone*.

Desta forma, será possível entender que tipo de informações os utilizadores estão a fornecer às organizações que disponibilizam os serviços através dos *Smartphones*. Posto isto, conseguiremos perceber se a população estudada sabe que tipo de informações está a disponibilizar aos vários tipos de organizações, ao usar o seu telemóvel, sendo, depois, possível determinar se a população em causa está pronta para ter uma vida transparente perante estas organizações.

3.3. Amostra

A amostra deste estudo são alunos de licenciatura do primeiro ano da escola ISTA do ISCTE. Numa primeira instância, são entrevistados 8 alunos do primeiro ano de quatro cursos (Arquitetura, Engenharia de telecomunicações de informática, Engenharia Informática, Informática e Gestão). O guião de entrevista elaborado para este efeito permite recolher os dados de forma a registar o comportamento que os alunos têm com o *Smartphone*, nas várias situações do dia-a-dia analisadas nesta investigação.

Após a entrevista, os 8 inquiridos preencheram o questionário elaborado, de forma a validar o questionário junto de um grupo representativo da população em estudo.

3.4. Guião do procedimento da entrevista

As entrevistas decorreram num ambiente calmo, dentro de uma sala de estudo, no ISCTE. O tempo de cada uma foi, aproximadamente, de 45 minutos. Estas foram conduzidas pelo investigador. Iniciaram-se com uma pequena introdução sobre o tema que a rodeia e seguiu-se o guião desenvolvido com as questões (apêndice E) para a entrevista.

3.5. Técnica de Análise de Dados Quantitativos

Adotar-se-á uma estratégia de investigação quantitativa, na qual se recolherá um conjunto de dados quantitativos, através das técnicas de entrevista e questionário.

Tendo em conta a natureza do estudo, adotar-se-á uma estratégia de investigação quantitativa, onde se recolherão dados quantitativos, através da técnica de questionário, com respostas fechadas. Estes questionários serão feitos a alunos do primeiro ano da escola ISTA do ISCTE, sendo estes a população em estudo para esta dissertação.

Para verificar alguns comportamentos do dia-a-dia destes utilizadores, serão feitas 8 entrevistas, duas por cada um dos seguintes cursos da escola ISTA: Arquitetura; Engenharia de telecomunicações de informática; Engenharia Informática; Informática e Gestão. Este pré-estudo é importante no sentido em que permite ter uma ideia concreta do comportamento destes estudantes com o *Smartphone*. Foi feita uma análise descritiva das entrevistas.

No mesmo momento, foi pedido aos participantes que preenchessem o questionário e dessem o seu feedback de imediato sobre as questões, de forma a se fazer a validação do

mesmo. Um segundo momento de validação do questionário ocorreu com o apoio de três professores que analisaram o questionário novamente e, num último momento, três colegas de mestrado fizeram também a validação do mesmo antes de este ser aplicado na população alvo.

A técnica de questionário fechado usada neste estudo implica seguir um guião que não permita aos participantes responder de forma vaga ou aberta, garantindo, assim, que não trazem informação extra à inicialmente desenhada, o que resulta numa amostra não-exploratória, mas que garante eficácia nos resultados pretendidos. Uma outra grande vantagem é a obtenção de respostas precisas e rápidas, de forma a conseguir um tratamento de dados mais preciso, o que permite, então, validar o estudo (Boni & Quaresma, 2005).

Pretende-se, desta forma, minimizar a variação das respostas dadas no questionário, com o objetivo de obter uniformidade na informação recolhida através do mesmo. Assim, conseguir-se-á um maior controlo sobre as respostas, ao mesmo tempo que se obtém a verificação do estudo. Embora perca algum aprofundamento e se reduza a exploração, assegurar a uniformidade na informação recolhida é imperativo, visto que se pretende garantir a possibilidade de replicação deste estudo em outros cenários, por todo o país, futuramente. Este tipo de questionário é adequado para ser replicado e poderá ser usado em outros estudos que cumpram os requisitos para o efeito.

Os dados quantitativos serão recolhidos com a técnica de questionário com perguntas de resposta fechada, onde os inquiridos terão de escolher entre as possíveis respostas que lhes são sugeridas. O questionário foi elaborado a partir da revisão de literatura, incluindo o modelo *TUM* aplicado neste estudo. Com este método de resposta fechada, também será possível obter mais facilmente respostas ao questionário, visto que os alunos não vão necessitar de escrever as respostas. Têm apenas de selecionar as respostas em forma de escolha múltipla, o que poderão fazer até mesmo através do seu *Smartphone*, em qualquer lugar com acesso à internet.

A possibilidade da obtenção de respostas rápida foi reconhecida como uma vantagem na aplicação da técnica de questionário. A escolha de alunos universitários do primeiro ano facilita a obtenção de respostas, pois o contacto entre o investigador e os docentes eleva a disponibilidade e mitiga a resistência destes alunos a participarem no preenchimento do mesmo. Deste modo, a amostra deste estudo é uma amostra por

conveniência, ainda que os participantes não sejam do conhecimento do investigador, o que garante a validade do estudo.

O questionário tem uma primeira parte onde são aplicadas as questões sobre os dados sociodemográficos (DS) e sobre o perfil tecnológico (PT) do inquirido. Na segunda parte, as perguntas, desenhadas com base nos estudos científicos analisados antes e ao longo da investigação, correspondem ao modelo *TUM*, o qual inclui os modelos da teoria do nível de adaptação (*ALT*), da teoria da dissonância cognitiva (TCD) e do modelo de aceitação (*TAM*). São aplicadas escalas do tipo *Likert*, entre 1 e 5, nas quais o valor 1 pode corresponder, por exemplo, a “Nada seguro” e o valor 5 a “Muito seguro”.

Escolheu-se a plataforma *Google Forms* para a elaboração deste questionário devido à sua simplicidade de utilização para a criação de questionários, ao facto de facilitar a distribuição dos questionários online através do mesmo e por ser completamente gratuito.

O facto de ser possível seleccionar, no *Google Forms*, a opção de obrigatoriedade de resposta a todas as perguntas, diminui a probabilidade de respostas inválidas, visto que elimina a possibilidade de submeter o questionário com algumas ou até todas as perguntas em branco. Este aspecto foi visto como uma função de valor acrescentado. Uma outra característica reconhecida como vantajosa é o facto de o *Google Forms* gerar, de forma automática, gráficos para a análise dos dados de cada pergunta, logo após o inquirido entregar o questionário. No entanto, o tamanho do link do questionário é um aspecto negativo, pelo que se optou por criar um *short link*, de forma a simplificar o mesmo e, conseqüentemente, permitindo uma maior facilidade no acesso ao questionário. Este link foi disponibilizado aos estudantes por email, através do *e-learning*, e também pessoalmente, por impresso, antes e depois das aulas dos alunos, nas instalações do ISCTE-IUL, de maneira a garantir a disponibilização do questionário ao maior número de alunos possível.

Estes dados serão analisados com o recurso à ferramenta *SPSS* e também com o estudo dos gráficos gerados pelo *Google Forms*. Com este estudo, será possível identificar e analisar os principais fatores com a utilização de dados privados que influenciem a utilização com os “*Smatphones*”.

Este estudo é um estudo não experimental, no qual as variáveis de interesse do mesmo são observadas relativamente ao modo como ocorrem naturalmente. Isto significa que é uma pesquisa de levantamento, onde os participantes respondem a um questionário de resposta fechada. Este tipo de pesquisas correlacionais não-experimentais são úteis para

avaliar se há ou não relação entre duas variáveis em populações. Neste caso, procura-se avaliar as relações entre o sexo, a geração (*i Generation* e *Digital Natives*) e o curso, e a segurança na utilização dos telemóveis.

O intervalo de anos da *i Generation* pode ser aplicado entre o ano 1991 e 2010 (Rosen, Carrier, & Cheever, 2010). No entanto, em Portugal, há estudos que indicam que só os jovens a partir do ano 2000 apresentam as características da mesma. Desta forma, encontramos a geração dos *Digital Natives* no intervalo entre os anos de 1991 a 2000, e a *i Generation* só a partir do ano 2000 (Messias, 2017).

O número da amostra é muito importante para o planeamento da investigação, pois tem impacto na qualidade do estudo e deve fazer parte de qualquer investigação. De forma a estabelecer este número de indivíduos que devem participar no estudo, é usado o cálculo da Fig. 12. Com este, garante-se a representatividade estatística do estudo.

$$n = \frac{N * Z^2 * p * (1-p)}{(N-1) * e^2 + Z^2 * p * (1-p)}$$

Figura 12 – Fórmula modelo da aceitação

Fonte: (Marcos, De, Aldemar, & Castro, n.d.)

O número de alunos inscritos por curso, no primeiro ano de licenciatura da escola ISTA do ISCTE, é o seguinte:

- Engenharia de telecomunicações e informática: 90 inscritos no primeiro ano
- Informática e gestão de empresas: 140 inscritos no primeiro ano
- Engenharia informática: 165 inscritos no primeiro ano
- Ciência de dados: 77 inscritos no primeiro ano
- Arquitetura: 74 inscritos no primeiro ano

Isto dá um total de 546 alunos inscritos no primeiro ano de licenciaturas da escola ISTA. Assim sendo, o tamanho da população em estudo é de 546, o que serve para calcular o tamanho mínimo necessário da amostra, de forma garantir um estudo com representatividade científica. Aplicando a fórmula da Fig.11, obtém-se, então, o cálculo abaixo.

Os parâmetros utilizados foram os seguintes: Número de amostra ($N = 546$); Nível de confiança para α igual a 0,05 ($Z = 1,96$); Margem de erro de 5% ($e = 0,05$);

$$\frac{546 * 1,96^2 * 0,5 * (1 - 0,5)}{(546 - 1) * 0,05^2 + 1,96^2 * 0,5 * (1 - 0,5)} = 225,74$$

O tamanho mínimo necessário da amostra é de 226 para um estudo com representatividade estatística com uma margem de erro de 5% e um nível de confiança de 95%, definido neste estudo. Como se conseguiu uma amostra de 317 neste estudo, pode-se concluir que o estudo tem representatividade estatística.

3.6. Análise quantitativa

Os dados quantitativos serão recolhidos com a técnica de questionário com perguntas de resposta fechada, onde os inquiridos terão de escolher entre as possíveis respostas que lhes são sugeridas. Estes dados serão analisados com o recurso de ferramenta *SPSS*. Com este estudo, será possível identificar e analisar os principais fatores com a utilização de dados privados que influenciem a utilização com os *Smartphones*.

3.7. Ferramenta de análise quantitativa SPSS

A ferramenta *SPSS*, que vai servir para analisar os dados recolhidos, é um software para a análise estatística de dados.

O *SPSS* é serve para a análises estatísticas, tais como, estatísticas descritivas, bivariadas e regressão, também possibilita a representação gráfica da análise feita.

Este software pode ser usado para dados experimentais ou observacionais. É considerado relativamente simples de usar graças à sua interface gráfica (Field, 2013).

Para as análises descritivas, neste estudo, foram aplicadas as técnicas da correlação de *V-Crámer*, o teste do Qui-Quadrado de independência, a razão de chances (*Odds Ratio*) e o coeficiente do *Alpha de Cronbach* (α).

3.8. Resultados

Este capítulo apresenta os dados recolhidos ao longo do estudo e a análise efetuada em função das questões de investigação e dos objetivos propostos nesta dissertação.

As entrevistas foram feitas presencialmente, depois dos participantes terem dado o seu consentimento para o uso das suas respostas no presente estudo.

O estudo quantitativo permitiu uma compreensão relativamente aos fatores que têm mais impacto na adoção e utilização do *Smartphone*, tendo havido, também, uma identificação dos riscos na utilização do aparelho. O comportamento dos utilizadores com os *Smartphones* que se identificou nesta análise permite a obtenção de indicadores sobre as alterações e melhorias o que os utilizadores desejam no tratamento dos seus dados de privados na utilização com o *Smartphone*.

A recolha de dados realizou-se durante o mês de maio de 2019, aquando foram recolhidos os dados das 8 entrevistas. Os dados recolhidos nas entrevistas foram registados no *Word* e trabalhados no *Excel* para análise. Os questionários foram realizados em setembro e outubro de 2019 com o registo dos dados feito no *Google Forms*. Foram exportados para análise no *Excel* e categorizados no programa de análise *SPSS*. O Sistema Operativo utilizado foi o *Windows 10*.

Capítulo 4 – Análise e discussão dos resultados

4.1. Recolha de dados

A recolha de dados foi planeada para encontrar respostas às questões de investigação, de forma a conseguir perceber quais os fatores que mais influenciam os participantes do estudo na utilização do *Smartphone*, em função da segurança da sua privacidade digital.

Na primeira parte da recolha de dados, entrevistaram-se 8 alunos do primeiro ano da escola ISTA do ISCTE (2 alunos de cada curso da escola: Arquitetura, Engenharia de telecomunicações de informática, Engenharia Informática, Informática e Gestão), uma vez que estes representam a população em estudo para a presente dissertação, de forma a compreender o comportamento que estes têm com o *Smartphone*, nas várias situações do dia-a-dia analisadas nesta investigação.

A distribuição dos elementos foi de 1 aluno do sexo masculino e 1 aluno do sexo feminino por cada curso. Com isto, foi possível recolher dados sobre o comportamento geral do dia-a-dia dos estudantes com *Smartphone*. Após a entrevista, e de forma a validar o questionário junto de um grupo representativo da população em estudo, perguntou-se aos estudantes a sua opinião quanto às questões que lhes foram colocadas, sendo-lhes também possível colocar diretamente as suas dúvidas e/ou sugestões sobre o questionário. Isto foi muito importante para mitigar a probabilidade de obter respostas erradas devido a uma má interpretação da pergunta.

Na segunda fase, depois de ter o questionário validado por outros investigadores, iniciou-se a fase de distribuição dos questionários para todos os alunos da escola ISTA com os seus respetivos cursos. A distribuição ocorreu através de vários meios, entre eles a distribuição por e-mail, a disponibilização do link no *e-learning* (na qual os estudantes podiam aceder ao questionário) e, por fim, a ida pessoal às aulas destes cursos, onde se apresentou a investigação e se pediu aos estudantes que participassem no estudo através do preenchimento do questionário. O último método foi o que mostrou claramente mais adesão por partes dos estudantes, visto que estes preencheram os questionários logo no momento.

Neste estudo, a recolha de dados foi realizada em contexto escolar, entre setembro de 2018 e janeiro de 2020, no ISCTE, e baseada na técnica de entrevista e questionário.

Trata-se de um estudo de natureza descritiva, documental, com abordagem quantitativa, que tem como propósito identificar se os estudantes aceitam os principais fatores de risco associados à utilização do *Smartphone*.

O objetivo desta análise é perceber se os estudantes universitários do primeiro ano da Escola de Tecnologias e Arquitetura (ISTA) do Instituto Universitário de Lisboa (ISCTE-IUL) sabem que a sua privacidade está em risco quando usam o *Smartphone*. Importa saber se percebem quais são os dados que disponibilizam às várias organizações de telecomunicações e também se tomam medidas para se proteger. Através de técnicas estatísticas, uma das fases deste estudo, responder-se-á às questões de investigação:

- a) Determinar o nível de confiança desta população com as organizações;
- b) Determinar se a população em estudo se sente segura relativamente à sua privacidade ao usar o *Smartphone* e as suas aplicações;
- c) Determinar o nível de satisfação do tratamento dos dados privados da população pelas organizações;
- d) Determinar o comportamento com o *Smartphone* ligado à internet, *GPS*, câmara, microfone;
- e) Determinar se a população estudada sabe que tipo de informações está a disponibilizar aos vários tipos de organizações;
- f) Determinar se a população em estudo aceita que as organizações tenham acesso a todos os dados privados introduzidos no *Smartphone*;
- g) Determinar se o *Smartphone* traz vantagens no dia-a-dia para o utilizador.
- h) Determinar a quantidade de utilização do *Smartphone*;
- i) Determinar se o utilizador é *digitally savvy*;
- 1) Determinar o tipo de informações que os utilizadores estão a fornecer às organizações que disponibilizam os serviços através dos *Smartphones*;
- 2) Determinar se a população estudada sabe que tipo de informações está a disponibilizar a terceiros, ao usar o seu telemóvel;
- 3) Compreender e identificar se é preciso tomar medidas futuras, de forma a proteger a privacidade digital de cada utilizador, com o propósito de, no futuro, garantir uma utilização dos *Smartphones* que deixe os utilizadores sem medo de expor a sua privacidade;
- 4) Perceber que utilização as pessoas fazem dos seus dispositivos móveis;
- 5) Determinar se a população aceita ter uma vida digital transparente no futuro.

As entrevistas e os testes do questionário, foram feitas presencialmente, nas instalações do ISCTE, na sala de estudo. Os questionários foram disponibilizados e recolhidos através da internet. Foi seguido um guião durante a realização das entrevistas conduzidas pelo investigador. As respostas, durante as entrevistas, foram registadas por escrito, visto que o guião não permitia respostas longas nem o acréscimo de informação extra por parte do entrevistado, num ambiente descontraído.

Momento do estudo	Recolha de dados	Calendarização
Definição inicial do estudo e revisão de literatura	Caracterização dos participantes para entrevista e questionário	Setembro de 2018 - Janeiro 2019
Desenvolvimento do Questionário e da Entrevista	Atividades de análise científica fundamentada	Janeiro de 2019 - Maio 2019
Convencer participantes a participar no estudo	Atividade de recruta	Maio 2019
Teste do Questionário com entrevistas (alterações e melhorias)	Entrevistas - 8 Participantes	Maio 2019
Recolha de dados	Questionário – Atividade online com <i>Google Forms</i>	Setembro 2019 - Outubro 2019
Análise de dados	Análise estatística - <i>SPSS</i>	Novembro 2019

Quadro 1 – Calendarização dos momentos e instrumentos de recolha de dados

4.2. Fase Quantitativa

4.2.1. Entrevista

As perguntas colocadas nas entrevistas foram construídas a partir da revisão de monografias e adaptadas para o estudo relacionado com o *Smartphone*. Foi criado um questionário com 18 perguntas de resposta fechada para este efeito, onde se seguiu um guião predefinido (apêndice D), que serviu para dirigir as entrevistas. Com o objetivo principal de perceber se a utilização do *Smartphone* feita pelos estudantes permite, ao mesmo, o registo de dados sensíveis ao longo do seu dia-a-dia.

As questões colocadas aos inquiridos no estudo em relação à segurança com o *Smartphone*, nas entrevistas, foram:

- Onde deixa o *Smartphone* quando está no restaurante em conversas privadas?
- Desliga o *Smartphone* quando está no Restaurante em conversas privadas?
- Desliga a internet quando está no Restaurante em conversas privadas?
- Onde deixa o *Smartphone* quando está na casa de banho?
- Desliga o *Smartphone* quando está na casa de banho?
- Desliga a internet quando está na casa de banho?
- Onde deixa o *Smartphone* em momentos íntimos como quando vai dormir?
- Desliga o *Smartphone* em momentos íntimos como quando vai dormir?
- Desliga a internet em momentos íntimos como quando vai dormir?
- Onde deixa o *Smartphone* quando está em casa?
- Desliga o *Smartphone* quando está em casa?
- Desliga a internet quando está em casa?
- Onde deixa o *Smartphone* quando está nas aulas ou no trabalho?
- Desliga o *Smartphone* quando está nas aulas ou no trabalho?
- Desliga a internet quando está nas aulas ou no trabalho?
- Onde deixa o *Smartphone* quando anda de transportes públicos?
- Desliga o *Smartphone* quando anda de transportes públicos?

- Desliga a internet quando anda de transportes públicos?

Os fatores para a escolha destas perguntas, fundamentais na base teórica, foram os fatores relacionados com a privacidade de dados recolhidos pelo *Smartphone*, nas situações de utilização diária. Assim, é possível obter uma compreensão mais profunda do comportamento do utilizador.

4.2.2. Conclusões das entrevistas

Com a análise dos dados recolhidos através das entrevistas aos oito inquiridos, foi possível retirar as conclusões previstas em relação ao uso do *Smartphone*. Uma delas foi o facto de apenas um único aluno, e apenas numa única situação, ter dito que se sentia mais seguro em desligar a internet, mais especificamente na situação em que vai à casa de banho.

Em todas as outras respostas não se observou qualquer preocupação dos alunos com o facto de o *Smartphone* poder registar dados sobre eles, nem tão pouco mostraram que se preocupam em evitar que o *Smartphone* possa, eventualmente, registar dados privados nas situações do dia-a-dia apresentadas durante as entrevistas. Mesmo em situações íntimas, na sua cama, referem que o *Smartphone* está sempre por perto. Um dos inquiridos afirmou mesmo que o *Smartphone* até está na cama ligado e conectado com a internet.

De forma a serem capazes de oferecer serviços pelos quais o utilizador tem a possibilidade de interagir com o seu dispositivo apenas utilizando a voz, tais como a *Siri* da *Apple* e a *Bixby* na *Samsung*, existe a necessidade do microfone estar sempre ativo para poder registar comandos de voz, mas, na verdade, regista tudo o que é dito, e só depois filtra o que são comandos ou não. Um caso mais recente aconteceu com a *Amazon*, onde foi descoberto que as gravações (comandos do utilizador) registadas e cujo sistema não entendia eram gravadas e reproduzidas a funcionários, para que estes, manualmente, introduzissem no sistema o que os utilizadores estavam a dizer, com o objetivo de melhorar o sistema. Este artigo, publicado por *Bloomberg*,¹ apesar de não ser de uma fonte científica, mostra os métodos aplicados pela *Amazon* para melhorar os seus sistemas de reconhecimento de voz. Dois funcionários desta empresa que falaram sobre estas técnicas usadas mencionaram que existem casos onde acreditam ter assistido

¹ Disponível em: <https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio>

a agressões sexuais e outros que disseram que partilham conversas privadas consideradas “engraçadas”, com outros funcionários, por chat. A *Amazon* reagiu depois de este caso vir a público, garantindo que vai implementar a opção do utilizador desativar, nas definições, este tipo de análise dos áudios registados pelos dispositivos, o que se pode encontrar nos termos de utilização da *Amazon* para os dispositivos que usam as funcionalidades de reconhecimento de voz com a assistente *Alexa*.

Outro aspeto igualmente importante prende-se com o facto dos *Smartphones* mais modernos terem as câmaras frontais ligadas. Em alguns casos, câmaras de infravermelhos, que permitem a visão noturna, para oferecer a funcionalidade de desbloquear o *Smartphone* através do reconhecimento facial, como é atualmente utilizado nas últimas gerações de *iPhones*.

Tendo em conta estes dois pontos anteriormente mencionados, podemos ver que existe a possibilidade de terceiros, com intenções maliciosas, entrarem nestes sistemas do *Smartphone* e registarem dados muito sensíveis dos utilizadores, se estes não tiverem certos cuidados.

Outro aspeto relevante é comparar o presente estudo com o trabalho de Anshari (2015), no qual este procurou saber os benefícios da recolha de dados através do *Smartphone* e os benefícios que o big data pode trazer neste contexto, com os dados recolhidos através de *Smartphones*.

“*Big data can capture patterns, trends, habit, and behaviour of smartphone users*” (Anshari & Alas, 2015).

Na recolha de dados no estudo de Anshari & Alas (2015), pode-se ver o comportamento dos utilizadores com os seus *Smartphones*, em várias situações do dia a dia. É interessante comparar estes resultados de Anshari & Alas (2015) - na figura 13 – com os deste estudo para compreender se existem semelhanças na utilização do *Smartphone*.

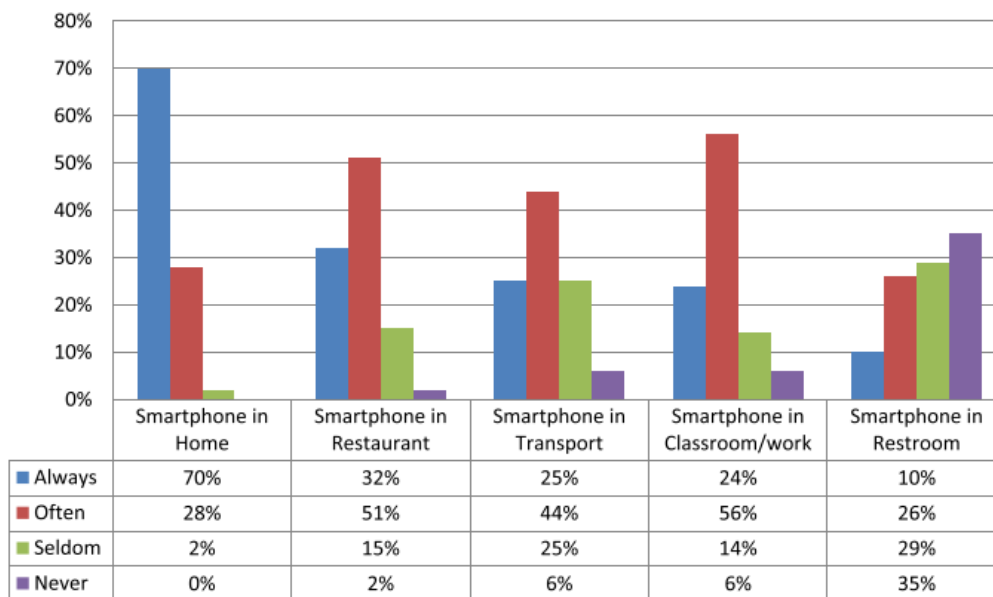


Figura 13 – Smartphone habits and personal feeling.

Fonte: (Anshari & Alas, 2015), Journal of High Technology Management Research 26

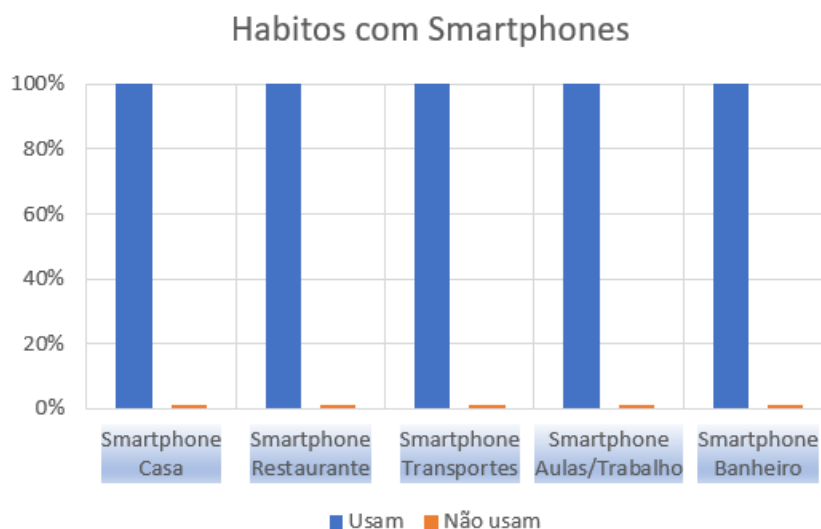


Figura 14 – Hábitos de utilização com Smartphones

Em ambos os estudos podemos concluir que 100% dos entrevistados usam o *Smartphone* em casa, o que prova que é possível a recolha de dados (*big data*) em casa de todos estes utilizadores, através do *Smartphone*.

Na situação onde os inquiridos usam o *Smartphone* na casa de banho, podemos encontrar diferenças, sendo que, neste estudo, todos afirmam que usam o *Smartphone* na casa de banho, em certas instâncias, o que não vai ao encontro do estudo de Anshari (2015). Neste, 35% afirma nunca usar o *Smartphone* na casa de banho. Não se consegue determinar se essa diferença surge pelo facto de o estudo de Anshari (2015) ter 44% dos

inquiridos com idade superior a 30 anos e 19% com idade superior a 55% ou se essa diferença está relacionada com o facto de os dois estudos terem grandes variações de gerações.

Em todas as situações incluídas no estudo, todos os alunos afirmam o uso do *Smartphone*. No estudo de Anshari (2015), tal não se confirma no restaurante, onde 2% afirma que não usa o *Smartphone*; nos transportes, onde 6% afirma não usar o *Smartphone*; e nas aulas ou trabalho, onde 6% afirma não usar o *Smartphone*.

No entanto, podemos concluir que a maior parte dos inquiridos, nos dois estudos, utiliza o *Smartphone* em todas as situações avaliadas e, com isto, existe a possibilidade de os *Smartphones* recolherem dados sobre eles em todas essas situações analisadas.

4.2.3. Questionário – Análise exploratória de dados (AED)

A técnica de inquérito por questionário e entrevista escolhida neste estudo é frequentemente usada no campo educativo, sendo aplicável também em outras áreas como foi o caso deste estudo (Tuckman, 2000).

A partir dos dados recolhidos por questionário, é possível que o investigador faça comparações e determine relações entre as respostas obtidas. Isto permite encontrar as características que os participantes têm em comum (Bell, 1993).

A planificação de um bom questionário é considerada uma tarefa difícil, até mesmo para investigadores com experiência. Como Bell (1997) menciona no seu livro, a “seleção do tipo de questões, na sua formulação, apresentação, ensaio, distribuição e devolução dos questionários” é algo que se deve fazer para ter um bom questionário.

Uma boa descrição para um questionário pode ser uma lista organizada de questões, com o objetivo da obtenção de informações de qualquer tema. A recolha de dados, aplicando o método de questionário, é diferente da recolha de dados obtida através dos métodos de entrevistas ou análise de documentos. Deve-se ter em conta as recomendações que existem para a formulação de um questionário. No entanto, não existe um método padrão para a aplicação de questionários. Cabe ao investigador definir perguntas adequadas à sua investigação, de forma a que os dados recolhidos possibilitem a resposta à pergunta de partida da investigação (Martyn Denscombe, 2001).

Existem duas maneiras para fazer análise de dados: exploratória e confirmatória. A análise de dados confirmatória acontece quando o investigador possui algum

conhecimento prévio de como as variáveis se comportam e se relacionam. Neste caso, como se possui pouco ou nenhum conhecimento sobre a estrutura dos dados e os seus comportamentos, é assim denominada como análise exploratória de dados (Sharma, 1996).

A análise exploratória de dados, também conhecida como análise descritiva, é o método que envolve a recolha, caracterização e apresentação de um conjunto de dados, de modo a descrever, de maneira simples e objetiva, as características deste conjunto (Mark L. Berenson, 1996).

De acordo com Morettin & Bussab (2017), na estatística, existem inúmeras ferramentas descritivas, como os gráficos, tabelas e medidas de síntese, como percentagens, índices e médias para organização dos dados, onde as mais utilizadas são séries estatísticas, conhecidas também por tabelas, que têm, por finalidade, resumir num quadro um conjunto de observações, conseguindo expor, de modo sintético, os resultados dos dados analisados relacionados com fatores como, tempo, local, fenómeno e especificação. Já os gráficos têm como objetivo principal produzir no leitor uma impressão mais rápida e viva dos dados de uma tabela.

A apresentação dos métodos utilizados para a realização da análise descritiva neste trabalho está representada em detalhe, no apêndice D, sendo estes o teste do Qui-quadrado de independência (χ^2), o coeficiente de *V Crámer* (*V*) e a razão de chances (RC).

Para a realização do estudo, foi feito um inquérito com os estudantes da Escola de Tecnologias e Arquitetura (ISTA) do Instituto Universitário de Lisboa (ISCTE-IUL).

Inicialmente, a amostra foi de 328 estudantes, com 329 respostas, do curso de Arquitetura, Ciência de Dados, Engenharia Informática, Engenharia Telecomunicações e Informática e de Informática e Gestão Empresarial. No entanto, um aluno negou-se inicialmente a responder ao questionário e voltou a repetir o mesmo mais tarde. De salientar, que 11 alunos foram retirados da amostra por não fazerem parte das gerações representativas e analisadas neste estudo (*Digital Natives* de 1991 a 2000 e *iGeneration* superior a 2000), logo, a amostra final foi de 317 estudantes.

Gil (2008) afirma que existem vários tipos de amostra aleatórias: a amostra simples, a amostra sistemática, a amostra estratificada, a amostra por conglomerados, entre

outras. No presente estudo, foi utilizada a amostra aleatória simples, na qual todos os sujeitos selecionados têm a mesma probabilidade de serem escolhidos (Gil, 2008).

O erro admitido no estudo foi de 3,64%, sendo considerado um erro baixo, uma vez que a população consiste em 546 alunos.

O instrumento de análise (*Google Forms*) permitiu a construção de folhas de cálculo eletrônicas no *software Microsoft EXCEL*, com todos os dados necessários para uma posterior análise, junto com um programa estatístico, *Statistical Package for the Social Sciences (SPSS)* versão 26, com a versão para estudantes e investigadores, que, por sua vez, geraram as análises multivariadas.

Os dados são filtrados, organizados e tabulados para depois serem submetidos a técnicas de organização e classificação, bem como a testes estatísticos para transformá-los em informações a serem analisadas e discutidas, à luz de um referencial teórico e de outras pesquisas.

O questionário aplicado contém três variáveis sociodemográficas do grupo 1, que são o sexo, a geração e o curso, enquanto as outras variáveis relacionadas foram as dos restantes grupos que dividem o questionário em dez partes. Segue-se a divisão dos grupos: perfil tecnológico - grupo 2; teoria do nível de adaptação - grupo 3; teoria da dissonância cognitiva - grupo 4; uso de smartphone - grupo 5; facilidade de uso percebida - grupo 6; utilidade percebida - grupo 7; intenção comportamental - grupo 8; uso real - grupo 9; confiança/segurança - grupo 10. O intuito é perceber o comportamento por sexo, curso e geração.

As respostas às perguntas foram organizadas em forma de escala, com opções de resposta, para obter a tendência das respostas no ponto central da mesma, em forma de escolha múltipla e também com perguntas dicotómicas.

Para verificar a fiabilidade do questionário, é importante analisar a consistência interna do mesmo, podendo esta ser verificada através do coeficiente *Alpha de Cronbach* (α) apresentado no anexo C.

O *Alpha de Cronbach* (α) calculado para os 26 itens dicotómicos foi de 46,00% ($\alpha = 0,46$) e para os itens politómicos foi de 58,00% ($\alpha = 0,576$), sendo considerado razoável pela maioria das escalas (Domingos Silva Júnior & José Costa, 2014; Hair Jr. et al., 2006; Landis & Koch, 1977).

Valor de alfa	Nível de consistência interna
< 0,00	Fraco
De 0,00 a 0,20	Pequeno
De 0,21 a 0,40	Razoável
De 0,41 a 0,60	Moderado
De 0,61 a 0,80	Substancial
De 0,81 a 1,00	Quase Perfeito

Figura 15 - Medição da concordância do observador para dados categóricos

Fonte: (Landis & Koch, 1977)

A consistência interna das dimensões investigadas confirmou (Tabela 60 apêndice C) que o instrumento é apto com os itens dicotómicos e politómicos, respetivamente, $\alpha = 0,459$ e $\alpha = 0,576$, e apresentou valores adequados de *Alpha de Cronbach*, com destaque para o grupo 10 (confiança/segurança) com $\alpha = 0,755$, grupo 9 (uso real) com $\alpha = 0,518$, grupo 8 (intenção comportamental) com $\alpha = 0,495$ e grupo 7 (utilidade percebida) com os itens dicotómicos e politómicos, respetivamente, $\alpha = 0,597$ e $\alpha = 0,476$), como mostra a Tabela 3. Ressalta-se que os itens do grupo 2 (perfil tecnológico) com $\alpha = 0,074$ e grupo 4 (teoria da dissonância cognitiva) com $\alpha = 0,139$ obtiveram os piores resultados, mostrando que possuem uma consistência interna muito pequena. Destaca-se que o grupo 5 (uso do *Smartphone*) não apresentou valores, pois o número de itens foi insuficiente para o cálculo.

4.2.4. Resultados dos questionários aplicados aos estudantes

Aqui, apresentam-se os resultados dos questionários recolhidos durante o ano letivo 2019/2020. Os participantes deste estudo foram alunos do primeiro ano de licenciatura da escola ISCTA do ISCTE, sendo a amostra final dos resultados avaliados de 317 estudantes. Em primeiro lugar, foi analisada a percentagem dos estudantes, na amostra deste estudo, por geração e sexo, como se verifica na tabela 1. O sexo feminino está representado com 20.59% na geração *Digital Natives* e com 79.41% na *iGeneration*, sendo que a maioria dos estudantes femininos pertence à *iGeneration*. No sexo masculino, foi verificada uma predominância de elementos da *iGeneration* (57.21%) comparativamente com os elementos masculinos da geração *Digital Natives* (42.79%). Existe uma predominância de estudantes que pertencem à *iGeneration* em ambos os

sexos, mas com mais representatividade no sexo feminino. Em seguida, foi feita a análise da distribuição dos estudantes por sexo e curso, e por geração por curso, como se pode verificar na tabela 2 e tabela 3, respectivamente.

Geração	Sexo	
	Feminino	Masculino
1991-2000	20.59	42.79
Maior que 2000	79.41	57.21
Total	100.00	100.00

Tabela 1 – Estudantes por Geração e Sexo

Curso	Sexo		Total
	Feminino	Masculino	
Arquitetura	26	22	48
Ciência de Dados	23	36	59
Eng. Informática	16	61	77
Eng. Telecomunicações e Informática	4	46	50
Informática e Gestão Empresarial	33	50	83
Total	102	215	317

Tabela 2 – Frequência de Alunos por Curso e Sexo

Curso	Geração		Total
	1991 a 2000	> 2000	
Arquitetura	17	31	48
Ciência de Dados	17	42	59
Eng. Informática	28	49	77
Eng. Telecomunicações e Informática	13	37	50
Informática e Gestão Empresarial	38	45	83
Total	113	204	317

Tabela 3 – Frequência de Alunos por Curso e Geração

O controle de qualidade da pesquisa foi feito através dos seguintes mecanismos:

- Crítica de consistência das respostas dos inquiridos;
- Auditoria da digitação/tabulação de dados;
- Controle de dados em digitação por meio de *software* específico (*SPSS*, *Excel* e *Google Forms*) para questionário aplicado.

O estudo conta com 215 (67,8%) alunos do sexo masculino e 102 (32,2%) alunas do sexo feminino, como se pode ver no gráfico 1.

1. Género

317 respostas

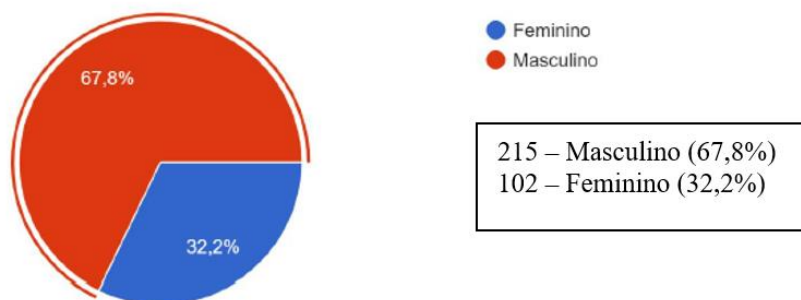


Gráfico 1 – Dados do Género

4.2.5. Análise e criação dos perfis dos estudantes

Numa primeira análise, de forma a poder determinar o perfil dos estudantes e definir a qual geração pertencem, foi analisado o intervalo de anos a que cada estudante pertence. Com esses dados, foi, então, possível identificar as características das gerações que estão presentes nesta investigação.

2. Ano de nascimento

328 respostas

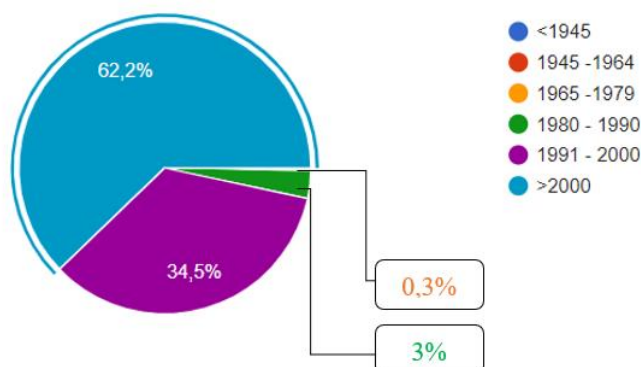


Gráfico 2 – Intervalos de anos de nascimento de amostra completa

De forma a poder comparar os resultados com a bibliografia, fez-se uma análise e criaram-se grupos, de maneira a separar os alunos por gerações.

Com a análise dos dados obtidos, pode verificar-se que, com uma percentagem de 62,2% (204), a maioria dos alunos nasceu depois do ano 2000 e pertence à *i Generation*, sendo que, no intervalo entre 1991 e 2000, se pode verificar uma percentagem de 34,5% (113 alunos), os quais pertencem à geração *Digital Natives*; para o intervalo entre 1980 e 1990, foi verificada uma percentagem de 3% (10 alunos), os quais pertencem à geração *Millenials* e, para o intervalo entre 1965 e 1979, foi verificado 0,3%, o que significa que apenas um aluno pertence a este intervalo e à geração X. Assim, foi determinado que as gerações *Millenials* e *Generation X* não são relevantes para este estudo. Com um número reduzido de alunos nestas duas gerações, não foi possível obter resultados representativos para fazer comparações. Para os restantes intervalos de anos, não foi verificado nenhum aluno no estudo. Tendo em conta o mencionado, foi criado o gráfico de distribuição das gerações relevantes para este estudo, como se pode verificar no gráfico 3.

2. Ano de nascimento

317 respostas

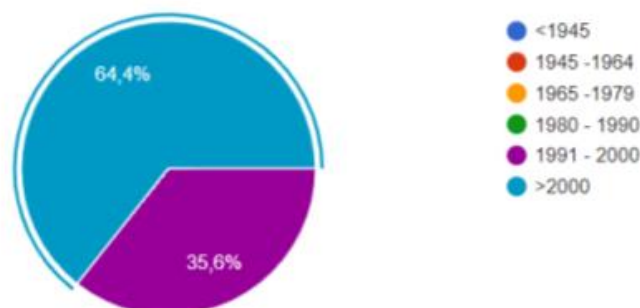


Gráfico 3 - Intervalos de anos de nascimento de amostra relevante para o estudo

Com a análise dos dados da amostra final, foi verificado que a maioria dos alunos (64,4%) nasceu depois do ano 2000 e pertence à *iGeneration*, sendo que, no intervalo entre 1991 e 2000, foi verificada uma percentagem de 35,6, que pertence à geração *Digital Natives*.

Na terceira questão do estudo, foi analisado o curso a que pertencem os estudantes, o que serve para a criação dos perfis dos alunos.

3. Indique o Seu Curso

317 respostas

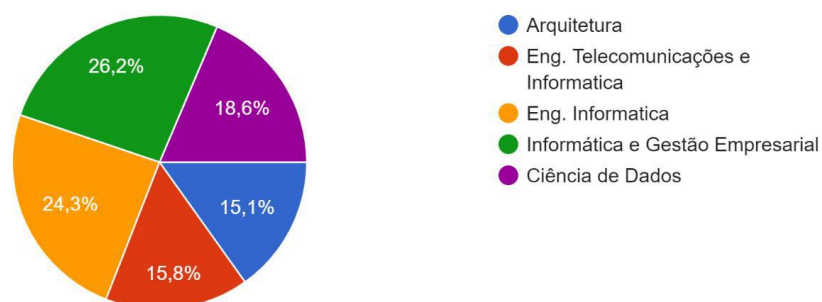


Gráfico 4 – Inquiridos por curso

Com a análise das respostas dos estudantes em relação ao curso que cada um frequenta, pode chegar-se à conclusão de que os estudantes se dividem equitativamente entre os cinco cursos representados neste estudo. As percentagens por cada curso são as seguintes: Informática e Gestão Empresarial - 26,2%; Engenharia Informática - 24,3%; Ciência de Dados - 18,6%; Engenharia de Telecomunicações e Informática - 15,8% e por fim Arquitetura - 15,1%.

O perfil tecnológico dos inquiridos foi a próxima análise. Com a revisão de literatura, foi criado um conjunto de dez perguntas para este efeito.

Depois da análise à primeira pergunta sobre o perfil tecnológico (gráfico 5, *c.f.* apêndice A), com um conjunto de ferramentas predefinido a partir da análise bibliográfica, percebeu-se que estes utilizadores usam maioritariamente a internet no seu *Smartphone*.

Os dados obtidos indicam que 277 dos inquiridos (87,4%) usam a internet no seu *Smartphone* para a participação nas redes sociais, 257 (81,1%) fazem uso da internet no *Smartphone* para ver vídeos, 233 (73,5%) para fazer pesquisa de conteúdos na internet, 232 (73,2%) para navegar por páginas de internet. Com 228 (71,9%) dos utilizadores a responder que usam a internet no *Smartphone* para consultar e-mail, completamos o grupo de respostas com uma taxa superior 70%. Nas seguintes atividades, verificou-se que as respostas dos utilizadores têm uma taxa inferior a 50%: 152 (47,9%) usam a internet no *Smartphone* para estudar; para jogar jogos ligados à internet obteve-se 150

(47,3%); para ver notícias online tem-se 133 (42%); para aprender, informalmente, através de tutoriais e vídeos tem-se 114 (36%); ver televisão online obteve 64 (20,2%); a opção “outros” obteve 41 (12,9); trabalhar colaborativamente obteve 36 (11,4%) e participar em fóruns obteve 22 (6,9%).

Tentando perceber há quanto tempo os estudantes têm um *Smartphone* pessoal, verificou-se (gráfico 6, *c.f.* apêndice A) que os inquiridos já o têm nos seguintes intervalos de anos: no intervalo de 4 e 6 anos são 39,7%, no intervalo de 7 e 8 anos são 31,9%, os que tem o *Smartphone* há mais de 8 anos são 22,7%, no intervalo de 1 e 3 anos são 5% e 0,6% tem um *Smartphone* pessoal há menos de um ano. Assim sendo, é possível concluir que 94,3% dos inquiridos tem um *Smartphone* há pelo menos 4 anos.

O facto apontado anteriormente permite concluir que a grande maioria, provavelmente, já tem algum conhecimento básico sobre o funcionamento do *Smartphone* e das suas funcionalidades ligadas à internet.

Em seguida, procurou-se identificar o comportamento dos estudantes em relação à forma de como se conectam à internet. A bibliografia aponta para o facto de as ligações com os *Smartphones* à internet elevarem o risco de alguém se infiltrar no sistema (Xiong & Jamieson, 2013), havendo uma maior probabilidade de sofrer um ataque, se a ligação à internet ocorrer a partir de uma rede pública (Delac et al., 2011).

Com os dados obtidos (gráfico 7, *c.f.* apêndice A), verificou-se que 96,8% dos inquiridos (37) usa a rede Wi-Fi privada de casa para se ligarem com o *Smartphone* à internet, 76,7% (243) usa a rede móvel privada do seu operador, 57,7% (183) usa redes públicas em lugares públicos, 47,9% (152) usa as redes Wi-Fi de amigos, 35,6% (113) usa a rede Wi-Fi disponível no trabalho e 15,1% (48) usa redes desconhecidas que oferecem internet gratuita.

Verificou-se, com estes resultados, que 15,1% dos inquiridos usa redes de *Wi-Fi* desconhecidas, o que representam um risco mais elevado para os seus dados privados. Isto pode significar que estes inquiridos não se importam, ou não têm conhecimento suficiente para tal, com os potenciais riscos que correm, ao se ligarem à internet, através de redes que lhes são completamente desconhecidas. Estas redes podem mesmo ser disponibilizadas por potenciais *hackers*. Redes *Wi-Fi* em lugares públicos (como em cafés), onde todos se podem ligar, têm uma segurança reduzida, na qual é mais fácil

apanhar pacotes de dados transmitidos pelos utilizadores. No entanto, verificou-se que mais de metade dos inquiridos (57,7%) acede a as estas redes em lugares públicos. Com isto, verificou-se que estes estudantes não parecem proteger-se da melhor maneira.

A pergunta sobre as aplicações que os inquiridos utilizam no seu *Smartphone* vai ao encontro de perceber quais as ferramentas usadas com o mesmo, partindo de um conjunto predefinido de aplicações, que vêm pré-instaladas no *Smartphone*, como acontece nos sistemas operativos da *Google (Android)* e da *Apple (iOS)*.

Com a observação dos dados (gráfico 8, *c.f.* apêndice A), verificou-se que todas as aplicações são usadas por mais de metade dos estudantes. As percentagens para as várias aplicações são as seguintes: aplicação de mensagens - 98,1%; aplicação de chamadas - 95%; aplicação da câmara - 94,6%; aplicação e-mail - 92,1%; aplicação para navegar na internet (*Web Browser*) - 89%; aplicação com *GPS* - 87,4%; aplicação do calendário - 72,6%; e aplicação agenda de contactos - 65,6%.

Através destas percentagens, é fácil perceber que as empresas que fabricam e produzem o *software* respetivo para estes dispositivos têm uma possibilidade muito abrangente de recolher dados sobre os seus utilizadores, se assim o quiserem fazer. Com aplicações como a de câmara, mensagens, chamadas e e-mail, pode existir uma possibilidade da grande maioria dos utilizadores serem controlados, seja pelos fabricantes destes dispositivos ou por terceiros que se infiltrem no sistema do *Smartphone*.

O *GPS*, com 87,4%, também mostra que existe a possibilidade, se terceiros acederem a estes dados registados pelo *Smartphone*, de descobrir onde o utilizador se encontra a cada momento.

Pretendeu-se, ainda, perceber se estes estudantes usam muito os seus *Smartphones* a partir da sua aplicação favorita (gráfico 9, *c.f.* apêndice A).

Depois da análise dos dados recolhidos, chegou-se à conclusão de que 75,1% dos inquiridos usa a sua aplicação favorita várias vezes ao dia online - pelo menos cinco vezes. No entanto, não estão sempre ligados à mesma. Interessante também é verificar que 8,8% dos alunos dizem estar sempre ligados à sua aplicação favorita, o que pode mostrar que este grupo de alunos pode estar constantemente a partilhar dados privados

que são registados por essa aplicação. Com 15,8%, obteve-se o grupo de estudantes que está, entre três a quatro vezes por dia, ligado online através da sua aplicação favorita. Um inquirido (0,3%) indica estar uma única vez online, por semana, na sua aplicação favorita *online*, e um inquirido respondeu que o faz com uma regularidade inferior à anterior.

No gráfico 10, (*c.f.* apêndice A) é possível observar se os estudantes têm o hábito de usar equipamentos adquiridos sem ler as instruções ou se querem perceber bem as funções dos equipamentos antes de os usar.

Com os dados recolhidos, observou-se que apenas 19,9% dos inquiridos indica ter o hábito de ler as instruções ou ler sobre o que se trata numa outra fonte. Isto significa que 80,1% dos inquiridos tem o hábito de abrir e usar o equipamento, sem ler as instruções ou o manual de instruções. Interessante é o facto de 39,4% responder que aprende por tentativa e erro, sem consultar um manual de instruções.

Estes dados podem apontar para o possível facto de 39,4% dos inquiridos não ter conhecimento suficiente de como os seus equipamentos funcionam e, possivelmente, não se aperceberem de que estão a disponibilizar dados sensíveis sobre a sua vida privada.

De forma a compreender o tipo de utilização que os estudantes fazem com o seu *Smartphone*, fez-se um conjunto de perguntas, tendo em conta o estudo de Messias (2017), que analisou este comportamento com estudantes nas redes sociais. Com a adaptação desta pergunta para a situação do *Smartphone*, procurou-se conhecer o tipo de informações que os estudantes incluem no perfil do *Smartphone* pessoal (gráfico 11, *c.f.* apêndice A).

Com a análise dos dados obtidos, verificou-se que a grande maioria dos estudantes usa o nome real - mais precisamente, 274 alunos, o que representam 86,4% da amostra. Este facto facilita a identificação mais precisa dos inquiridos por parte das organizações que conseguem acesso a estes dados. O endereço de e-mail é incluído por 242 estudantes (76,3%). Esta proporção é bastante diferente da obtida no estudo de Messias (2017), que obteve 28,9% de estudantes a afirmar que inclui o e-mail na sua rede social. Este facto pode ser um indicador de que os estudantes se sentem mais à vontade em incluir o seu e-mail no seu *Smartphone* do que nas redes sociais. Mais de metade dos estudantes

inclui o seu número de telefone - 200 (63,1%) - e fotografias pessoais - 197 (62,1%) -, no perfil da sua conta do *Smartphone*. Todos os restantes dados incluídos nesta pergunta obterão uma taxa inferior a 50%: naturalidade - 117 (36,9%) -, fotos de outros - 84 (26,5%) -, Local de residência - 54 (17%) -, estado civil - 30 (9,5%) -, endereço IM (*Instante Message*) - 24 (7,6%) -, outros - 12 (3,8%) - e orientação política obteve zero (0%).

Em comparação com a bibliografia, estes dados revelam que as afirmações de Messias (2017) se confirmam também nos *Smartphones*, sendo a existência de perfis detalhados menos frequente. Apesar de grande parte dos perfis não serem muito detalhados, a maioria dos estudantes inclui o nome real, o e-mail, o número de telemóvel e fotografias pessoais. Isto permite concluir que é possível obter perfis da maioria dos estudantes com este tipo de dados, apenas sendo necessário aceder aos dados incluídos no *Smartphone* pessoal dos inquiridos.

Perceber se os estudantes têm algum conhecimento sobre terceiros acederem aos seus dados registados através do *Smartphone* é importante para este estudo. Um estudo interessante sobre a criação de perfis de utilizadores refere que, através dos gestos que fazem no uso do seu *Smartphone*, ao navegar nas páginas da internet, é possível fazer uma autenticação baseada em 21 categorias diferentes, como velocidade e direção dos gestos e tempo de toque com o ecrã por cada vez que clica (Meng et al., 2018).

Com a recolha destes dados, parece ser possível obter perfis de autenticação sem os utilizadores se aperceberem.

“For user authentication on phones, there is a need to deploy a biometric system that can continuously collect raw data, extract features and conduct profile matching.” (Meng et al., 2018).

O objetivo da pergunta (gráfico 12, *c.f.* apêndice A) é perceber se os estudantes têm conhecimento da possibilidade de os seus dados privados, registados pelo *Smartphone*, estarem a ser utilizados por terceiros.

Na análise destes resultados, pode-se concluir que 74,1% dos estudantes afirma saber que os seus dados estão a ser usados por terceiros, enquanto 25,9% dos estudantes respondeu que não o sabe.

A grande maioria afirma ter conhecimento no que diz respeito a terceiros usarem os dados que o seu *Smartphone* regista. Isto pode ser um indicador de que estes estudantes aceitam o facto de existirem terceiros a utilizar os seus dados registados no dia a dia, pelo *Smartphone* pessoal. Por outro lado, os restantes 25,9% de alunos que respondeu “não” na presente questão, pode servir de indicador de que pelo menos um quarto dos estudantes não sabe que os seus dados são utilizados por terceiros ou, então, afirma que sabe que os seus dados recolhidos pelo *Smartphone* não são utilizados por esses.

Os termos de aceitação das tecnologias implicam, muitas vezes, o acesso a dados de posicionamento através do *Smartphone*. A seguinte pergunta (gráfico 13, *c.f.* apêndice A) foi ao encontro de perceber se os estudantes aceitam os termos de aceitação, quando estes implicam o acesso aos dados de posicionamento do *Smartphone*.

Num estudo de Obar & Oeldorf-Hirsch (2018), com o título “*the biggest lie on the internet*”, os autores chegam à conclusão de que 97% aceitava os termos de utilização. Note-se que 86% dos inquiridos leram os termos de utilização em menos de um minuto e, em média, um adulto necessitaria de 15 a 17 minutos para ler o documento completo. Para a apólice de privacidade, os inquiridos usaram 73 segundos, sendo que, em média, seriam necessários 29 a 32 minutos - 93% aceitaram a apólice de privacidade.

Isto mostra que é praticamente impossível que estes inquiridos tenham lido os documentos por completo e, com isso, provavelmente não seja possível estes terem um bom conhecimento relativamente ao que estão a aceitar.

“*All participants were presented the TOS and had an average reading time of 51 seconds.*” (Obar & Oeldorf-Hirsch, 2018).

Analisando os dados obtidos, chega-se à conclusão de que 74,8% dos utilizadores aceita os termos de utilização, mesmo quando sabem que estes implicam a permissão do acesso aos dados de posicionamento do *Smartphone*. Com isto, percebe-se que a grande maioria destes estudantes está disposta a partilhar os seus dados de posicionamento, o que torna possível a criação de perfis dos mesmos sobre os locais que frequentam.

Pelo menos um quarto dos estudantes afirma não aceitar os termos de aceitação, se estes implicarem o acesso aos dados de posicionamento do seu *Smartphone*.

Tendo em conta o estudo de Obar & Oeldorf-Hirsch (2018), é possível que, mesmo assim, os inquiridos que afirmam não aceitar os termos de aceitação, quando implicam o acesso aos dados de posicionamento, aceitem os termos de aceitação, sem se aperceberem de que estes implicam o acesso a esses dados, devido a uma leitura parcial do documento.

De forma a perceber até que ponto os estudantes sentem que o *Smartphone* afeta os estudos, recolheu-se a opinião dos mesmos sobre este tópico (gráfico 14, *c.f.* apêndice A), o que também ajuda a perceber se os *Smartphones* trazem vantagens aos estudantes no dia a dia e se isto pode ou não contribuir para uma maior utilização do *Smartphone*.

Ao analisar as respostas dos estudantes, verificou-se que 41% respondeu que o *Smartphone* afeta os estudos de forma ligeiramente negativa e 25,9% respondeu o oposto, afirmando que o *Smartphone* afeta os estudos de forma ligeiramente positiva. 12,3% dos estudantes afirma que o *Smartphone* não tem qualquer impacto nos seus estudos, pelo que este grupo é relativamente pequeno. A percentagem de estudantes que afirma que o *Smartphone* afeta os seus estudos de forma bastante positiva é de 14,2% e com 6,6% obteve-se a resposta que aponta que o *Smartphone* afeta os estudos de forma bastante negativa.

Com isto, percebeu-se que os estudantes têm formas diferentes de utilização do *Smartphone* relativamente aos seus estudos. Uma grande parte dos alunos (41%) afirmou que o *Smartphone* afeta os seus estudos de forma ligeiramente negativa e pelo menos um quarto afirmou que o *Smartphone* afeta os estudos de forma ligeiramente positiva.

Estes resultados são diferentes dos resultados obtidos por Messias (2017), no estudo relativo às redes sociais, podendo concluir que, neste aspeto, o *Smartphone* não afeta os estudantes nos estudos de forma semelhante com o que acontece nas redes sociais. No estudo de Messias (2017), 24% indicou que as redes sociais afetam os seus estudos de forma bastante positiva, o que corresponde a uma percentagem bastante superior à obtida para o *Smartphone* - 14,2%. Também se observou uma grande diferença no que diz respeito ao aspeto de afetar os estudos de forma ligeiramente negativa, onde 41% dos estudantes diz ser afetado pelo *Smartphone* dessa maneira. Relativamente às redes sociais, no estudo de Messias (2017), apenas 11% respondeu da mesma forma, o que resulta numa diferença quase quatro vezes inferior em relação ao *Smartphone*.

4.2.6. Análise dos resultados relativamente à Teoria do Nível de Adaptação

A teoria ALT² é uma componente importante no modelo TUM³, utilizado nesta investigação. As próximas cinco perguntas vão ao encontro de perceber as expectativas iniciais, que servem como base de comparação do nível de adaptação dos estudantes.

Em seguida, foi analisada a opinião dos estudantes, de forma a perceber se consideravam que a utilização das aplicações de comunicação no *Smartphone* teria riscos para a sua privacidade, antes de terem o aparelho (gráfico 15, *c.f.* apêndice A).

Com a análise dos dados obtidos, observou-se que 32,2% considera que a utilização tem poucos riscos, 30,3% considera que tem bastantes riscos, 29% considera que tem um risco neutro, 5% considera que não tem riscos nenhuns e 3,5% considera que tem muitos riscos.

Num estudo feito por Vallina-Rodriguez & Sundaresan (2017), verificou-se que mais de 70% das aplicações de *Smartphone* analisadas no estudo reporta dados privados a terceiros, para entidades como Google Analytics, Facebook Graph API ou Crashlytics, que permitem localizar os utilizadores e construir perfis muito mais completos sobre os seus dados digitais.

A maioria dos estudantes parece ter conhecimento relativamente à existência de riscos de privacidade relacionados com as aplicações de comunicações utilizadas com os *Smartphones*, sendo que 95% dos utilizadores já considerava que a utilização destas aplicações teria, pelo menos, poucos riscos para a sua privacidade.

Em seguida, analisou-se a perceção dos estudantes, de forma a verificar se consideravam que poderiam confiar a partilha de informação inerente à utilização das aplicações de comunicação, no *Smartphone*, necessárias ao funcionamento deste, previamente à sua obtenção (gráfico 16, *c.f.* apêndice A).

Num estudo feito por Dwyer, Roxanne Hiltz, Passerini, & Roxanne (2007), onde se compararam as redes sociais MySpace e Facebook, os autores não encontraram

² Teoria do Nível de Adaptação

³ Modelo de Uso de Tecnologia

diferenças significativas da confiança dos utilizadores, sendo que admitem ser difícil perceber a função da confiança e privacidade com as redes sociais.

“This makes it difficult to understand the role of privacy and trust within social networking sites” (Dwyer et al., 2007).

É interessante comparar e verificar se, para os *Smartphones*, os resultados são similares. Na análise dos resultados obtidos, verificou-se que 37,9% dos estudantes considerava confiar pouco, 36,9% tinha uma opinião neutra, 13,9% considerava confiar bastante, 11% considerava não confiar e 0,3% considerava confiar muito na partilha de informação inerente à utilização das aplicações necessárias ao funcionamento do *Smartphone*. Tendo em conta estes resultados, verificou-se que pelo menos 48,9% dos estudantes confiava pouco ou não confiava na partilha inerente à utilização das aplicações necessárias ao funcionamento do *Smartphone*. Visto que a partilha destas informações é inerente ao funcionamento do telemóvel, isto pode significar que estes estudantes confiam pouco no *Smartphone*. Uma percentagem grande - 36,9% - corresponde à resposta na qual afirmam que tinham uma opinião neutra, significando que estes não tinham a certeza se deviam ou não confiar. Isto pode ser um indicador da falta de conhecimento dos utilizadores quanto ao tipo de informações que são inerentes para o funcionamento do *Smartphone*.

Na questão representada no gráfico 17 (c.f. apêndice A), foi analisado se os estudantes, antes da aquisição do *Smartphone*, consideravam que a utilização do equipamento iria trazer riscos de privacidade relativamente aos dados móveis que iriam partilhar com o mesmo.

Esta pergunta foi criada depois de analisar o estudo de Lell & Nohl (2018), o qual mostra possíveis vulnerabilidades que os *Smartphones*, com o sistema operativo “*Android*”, têm relativamente a lacunas que surgem a partir das atualizações. Na análise binária feita, concluiu-se que, apesar de ser mais difícil do que o esperado, é possível que *hackers* tirem proveito dessas lacunas ocorridas nas atualizações. Com certos fabricantes de *Smartphones*, as atualizações não se verificaram, algumas vezes, ao nível prometido, significando uma vulnerabilidade para estes dispositivos. Assim, é fácil de perceber que podem existir riscos de privacidade ao utilizar os *Smartphones*, como no caso investigado com o sistema *Android*, para os utilizadores.

Com os dados recolhidos, verificou-se que 36,9% dos estudantes considerava haver alguns riscos, 25,9% considerava haver um risco neutro, 23% considerava haver poucos riscos, 8,8% não considerava haver riscos e 5,4% considerava haver muitos riscos de privacidade relativamente aos dados móveis que iria partilhar - isto previamente à aquisição do *Smartphone*. Uma conclusão interessante é que 91,2% dos inquiridos afirmou, pelo menos, considerar poucos riscos de privacidade relativamente aos dados que iria partilhar, depois de adquirir um *Smartphone* via dados móveis, sendo, assim, possível encontrar uma certa incerteza e desconfiança, por parte da maioria dos estudantes, na utilização do *Smartphone*. É também um possível indicador de que o problema da segurança dos dados privados dos utilizadores relacionados com os *Smartphones*, tais como os identificados no estudo de Lell & Nohl (2018), é bastante conhecido por estes estudantes do primeiro ano de Licenciatura da escola ISTA do ISCTE.

A câmara do *Smartphone*, que tem a característica de produzir imagens, apresenta um risco elevado de privacidade, caso seja acedida por terceiros, sem que os utilizadores se apercebam. No estudo de Deshpande & Dharmadhikari (2016), onde são analisadas e discutidas possíveis medidas para proteger *Smartphones*, com o sistema *Android*, de espionagens através da câmara, percebeu-se que a integração de tecnologias, num processo de certificação de aplicativos, requer a superação de desafios logísticos e técnicos. Também se fala da função que a possível espionagem, através da câmara do *Smartphone*, pode significar, sendo evidente que existem potenciais riscos de privacidade ao usar *Smartphones* com câmaras integradas.

Na análise dos resultados recolhidos sobre esta questão (gráfico 18, *c.f.* apêndice A), foi verificado que 30% dos estudantes considerava haver poucos riscos, 22,7% não considerava nenhum risco, 19,9% considerava haver um risco neutro, 20,2% considerava haver alguns riscos e 7,3% considerava haver muitos riscos ao usar um *Smartphone* com câmara, previamente a ter um. Estes resultados significam que 77,3% dos estudantes que responderam ao questionário considerava, pelo menos, a existência de poucos riscos de privacidade ao utilizar um *Smartphone* com câmara. Isto parece ser um possível indicador de que existe uma certa desconfiança destes utilizadores perante as organizações que oferecem os serviços de comunicações através dos *Smartphones*. Note-se que parece que estes estudantes já tinham um certo conhecimento, antes de usar o *Smartphone* com câmara, de que este poderia apresentar riscos para a sua privacidade.

Na última pergunta (gráfico 19, *c.f.* apêndice A) deste estudo, relacionada com a teoria do nível de adaptação, perguntou-se aos estudantes se estes, previamente à aquisição do seu *Smartphone*, consideravam necessário instalar uma aplicação para manter o seu direito à privacidade com a utilização do mesmo.

Num estudo de Warren & Brandeis (1890), o autor fala sobre o direito da privacidade e as leis que protegem ou não cada indivíduo nesse sentido, até mesmo no que se diz ser a violação de honra. Pode-se ver que, há 129 anos, os problemas de privacidade e as definições das leis eram um tema importante para proteger a privacidade e a propriedade intelectual de cada indivíduo. Tudo isto parece que se volta a repetir no século XXI, devido às grandes invenções da tecnologia nos últimos anos, onde estão a aparecer leis que vão ao encontro da proteção de cada indivíduo na sua privacidade e propriedade digital. Uma delas é a lei de proteção de dados (RGPD), muito falada pelos *media*, em Portugal e na união europeia. Esta entrou em vigor no dia 25 de maio de 2018, na união europeia, com o objetivo de proteger os dados privados dos utilizadores e limitar o acesso de terceiros a estes dados, sem a respetiva autorização.

O estudo de Delac et al. (2011b) mostrou que os recentes avanços nas tecnologias móveis trouxeram um foco para os ataques maliciosos a *Smartphones*. Em sistemas operativos como o *Android*, é possível instalar aplicações de terceiros e de fontes desconhecidas, o que significa que os utilizadores têm de julgar o risco, ao baixar e instalar as aplicações para não sofrerem ataques no seu dispositivo. Assim, basta que o utilizador julgue de forma errada o risco para que terceiros possam ter acesso aos dados do seu *Smartphone* (Delac et al., 2011).

“The trends show a severe increase in mobile malware as many threats, designed for PC operating systems, migrate to mobile platforms.” (Delac et al., 2011).

Tendo conhecimento destes factos, procurou-se perceber se os estudantes, mesmo antes de comprarem o *Smartphone*, consideravam necessário instalar uma aplicação como um antivírus, para proteger a sua privacidade no uso do *Smartphone* (gráfico 19, *c.f.* apêndice A).

Com a análise dos dados recolhidos, verificou-se que 33,8% não considerava necessário, 26,2% considerava a necessidade neutra, 20,5% considerava pouco

necessário, 14,2% considerava bastante necessário e 5,4% considerava muito necessário instalar uma aplicação para proteger a sua privacidade no *Smartphone*.

Apenas 19,6% dos inquiridos respondeu que considerava, pelo menos, bastante necessário instalar uma aplicação para proteger a sua privacidade com a utilização do *Smartphone*. A maioria dos estudantes não considerava bastante necessária esta instalação.

4.2.7. Análise dos resultados relativamente à Teoria da Dissonância Cognitiva

No próximo setor do questionário, o grupo 4, foram feitas perguntas relacionadas com a teoria da dissonância cognitiva. Esta teoria é uma componente do modelo *TUM*, usado neste estudo e muito importante para as conclusões finais.

Na primeira questão deste setor, analisou-se se os estudantes tiveram momentos onde se preocuparam com a sua privacidade ao utilizar o *Smartphone* (gráfico 20, c.f. apêndice A).

O estudo de Levin (1957) fala sobre a dissonância e quando esta pode ocorrer.

Aplicando no caso da tecnologia, a dissonância cognitiva pode ocorrer antes e depois das principais decisões de compra. Esta surge frequentemente quando as alternativas consideradas apresentam vantagens e desvantagens para a compra da tecnologia. Isto apresenta um conflito cognitivo de decisão para o potencial comprador da tecnologia, o que pode levar a um atraso ou até mesmo a uma não compra neste processo.

No estudo de Levin et al. (2013), no qual se compararam os níveis de dissonância na interação de humanos com robôs e na interação de humanos com humanos, os investigadores observaram que a dissonância de humanos com um parceiro robô foi mais elevada. A investigação deste estudo foi um bom exemplo da interação entre humanos e tecnologia, o que serviu para ser adaptada, no presente estudo, aos *Smartphones*. As seguintes oito perguntas vão servir para tentar medir os níveis de dissonância dos utilizadores com os *Smartphones*, através da teoria de dissonância cognitiva.

Ao avaliar os dados obtidos, verificou-se que a grande maioria já teve momentos onde se preocupou com a sua privacidade, ao utilizar o *Smartphone* - 77,9% respondeu

que sim, enquanto 22,1% respondeu não ter tido esses momentos. Isto pode ser um indicador de que existem certas situações de privacidade, nas quais os inquiridos se sentem ameaçados pelos *Smartphones* relativamente à sua privacidade, ficando preocupados relativamente a um possível registo do *Smartphone*, no que diz respeito a certos eventos da sua vida privada. Mais uma vez, observaram-se indicadores de um certo nível de desconfiança perante as organizações que disponibilizam os serviços de comunicações no *Smartphone*, havendo uma maioria que indica que não se sente seguro, em certas alturas, ao utilizar o telemóvel. Estas inseguranças podem ocorrer pelo facto de os utilizadores não saberem exatamente o que o *Smartphone* regista, para onde envia os dados e para o que estes são utilizados.

Em seguida, com o propósito de perceber se o nível de dissonância seria tão elevado de forma a que os estudantes se arrependeram de ter comprado um *Smartphone*, procurou-se saber se estes voltariam a comprá-lo, se pudessem voltar atrás (gráfico 21, *c.f.* apêndice A).

Na análise das respostas obtidas, observou-se que a grande maioria - 96,2% - voltaria a comprar um *Smartphone* e apenas 3,8% indicou que, se pudesse voltar atrás, não o voltaria a comprar. Isto mostra que, apesar da percentagem alta de inquiridos que indica uma certa preocupação com a sua privacidade ao usar o *Smartphone*, estes não parecem estar dispostos a abdicar do mesmo e, por isso, preferem viver com o risco de a sua privacidade digital estar potencialmente a ser usada para fins desconhecidos e maliciosos.

Isto revela que as organizações que vendem e disponibilizam os serviços para *Smartphones* podem continuar a recolher os dados privados dos utilizadores, sem que a grande maioria deles pare de os comprar por esse motivo. A grande parte dos inquiridos parece optar por viver com o risco de não ter privacidade digital perante as organizações e potenciais desconhecidos, ao invés de abdicar dos *Smartphones* e de todas as suas ferramentas e funcionalidades.

Em seguida, procurou-se perceber se as expectativas dos estudantes relativamente a algumas funcionalidades do *Smartphone* seriam consistentes com a realidade, depois da utilização das mesmas (gráfico 22, *c.f.* apêndice A).

Na observação dos dados, verificou-se que 49,8% dos inquiridos indicou ter um nível de dissonância perante as expectativas de algumas funcionalidades com a realidade, depois da utilização das mesmas. 50,2% dos inquiridos indicou que as expectativas e a realidade eram consistentes. Verificou-se que, quase metade dos inquiridos, em algumas funcionalidades do *Smartphone*, teve inconsistências com as expectativas, antes da utilização.

Em seguida, procurou-se saber se os inquiridos sempre tiveram a certeza de como é a utilização do *Smartphone* (gráfico 23, c.f. apêndice A).

Com os dados recolhidos dos estudantes, foi observado que 62,5% indicou ter sempre a certeza de como era a utilização do *Smartphone* e 37,5% indicou o contrário, dizendo que não teve sempre a certeza de como era utilização do aparelho. Assim, verificou-se que a grande maioria, pelo menos, acha que sempre soube como era a utilização do *Smartphone*. Isto pode ser um indicador de que estes estudantes são *digitally savvy*, tendo conhecimento de como utilizar as tecnologias e sabendo avaliar corretamente as vantagens que o *Smartphone* lhes oferece no dia-a-dia.

Perceber se os estudantes confiaram no seu *Smartphone* no passado é muito vantajoso para este estudo, uma vez que se pode avaliar se os estudantes também têm ocasiões nas quais sentem poder confiar no *Smartphone*.

Ao olhar para os dados recolhidos sobre esta questão, no gráfico 24 (c.f. apêndice A), verificou-se que 80,8% indicou que confiou no *Smartphone*, sendo, assim, claro que a grande maioria já ofereceu algum nível de confiança ao seu *Smartphone*. Por outro lado, 19,2%, não confiou no seu *Smartphone* no passado.

Perceber se os estudantes se sentiram confortáveis ao usar o *Smartphone* no passado ajuda a perceber se estes se preocupam muito ou não com os dados privados que introduzem no seu *Smartphone* (gráfico 25, c.f. apêndice A) e com as funcionalidades usadas através do mesmo.

Na análise dos resultados obtidos, verificou-se que a grande maioria se sentiu confortável ao usar o *Smartphone* - 94,6% respondeu que sim e apenas 5,4% respondeu que não. Este resultado ajuda a explicar a relação do utilizador com o *Smartphone*, sendo

que o facto de se sentir confortável com o seu uso significa uma maior satisfação com a tecnologia.

Verificar se os estudantes acham que utilizaram corretamente o *Smartphone* ajuda a perceber se estes sabem usar as funcionalidades de um modo adequado e se percebem como o *Smartphone* funciona, sendo que também pode servir como indicador para perceber se estes são *digitally savvy* (gráfico 26).

Com a grande maioria de 90,5% a responder que acha que utilizou corretamente o *Smartphone*, podemos verificar que apenas 9,5% indica tê-lo utilizado incorretamente. A percentagem dos estudantes que diz não ter utilizado de uma forma correta o seu *Smartphone* é baixa, sendo possível concluir que, provavelmente, a grande maioria dos estudantes sabe trabalhar corretamente com o *Smartphone* e tem o conhecimento necessário para o utilizar adequadamente. Este resultado também é um indicador de que a grande maioria dos estudantes é *digitally savvy*.

Interessante também é perceber se os estudantes estão dispostos a desistir da utilização do *Smartphone*, conhecendo os riscos de segurança que estes têm. Este aspeto permite obter indicadores, de forma a perceber se os estudantes aceitam que as organizações ou terceiros tenham acesso aos dados do *Smartphone*.

Com os dados recolhidos sobre este tópico (gráfico 27, *c.f.* apêndice A), foi observado que a grande maioria dos estudantes, mais precisamente 96,5%, afirmou não deixar de utilizar o *Smartphone*, conhecendo os riscos de segurança. Mesmo não terem sido apresentados riscos neste inquérito, ou seja, mesmo estes não tendo conhecimento de quais os riscos de segurança envolvidos, responderam que não vão deixar de usar o *Smartphone*, o que pode significar que, independentemente dos riscos que potencialmente existam, a grande maioria dos estudantes diz que usaria o *Smartphone*. Estes resultados permitem entender o potencial poder que as organizações têm sobre os utilizadores, uma vez que 96,5% dos utilizadores afirma continuar a utilizar os *Smartphones*, ainda que tenha riscos de segurança desconhecidos. Apenas 3,5% indica que não vai continuar a usar o *Smartphone*, o que demonstra que estes, provavelmente, têm um maior conhecimento relativamente aos riscos envolvidos na utilização dos *Smartphones* e/ou dão mais importância à sua privacidade digital.

4.2.8. Análise dos resultados relativamente à utilização do *Smartphone*

No próximo setor do questionário, que corresponde ao grupo 5, analisou-se a utilização que os estudantes dão ao seu *Smartphone*. Perceber com que frequência e qual a quantidade de tempo que os estudantes utilizam o *Smartphone* serve como indicador para medir a dependência e o nível de integração que estes telemóveis têm na vida dos estudantes.

Visto que a amostra é composta por universitários, perceber se estes tiram partido do *Smartphone* para o meio académico é interessante (gráfico 28, *c.f.* apêndice A). O *Smartphone* tem o potencial de ser uma ferramenta conveniente em muitas situações na faculdade, visto que é um dispositivo muito portátil e de fácil acesso, e permite aceder a informações académicas sem grande esforço e com muita rapidez.

A grande maioria de 95,6% dos estudantes indica que utiliza o *Smartphone* para o uso académico. Isto mostra que este aparelho é utilizado pela maioria dos estudantes e que este realmente parece trazer vantagens em certas situações do uso académico, como era previsto por se tratar de um dispositivo com uma portabilidade e acessibilidade grandes. Mais uma vez, também permite obter um indicador de que a maioria destes estudantes são *digitally savvy* e que usam o *Smartphone* em muitas situações e vários fins, como se tem observado ao longo desta análise de dados. Apenas 4,4% respondeu que não utiliza o *Smartphone* para fins académicos.

No estudo de Ferreira (2014), sobre a aceitação da tecnologia relacionada com o *Facebook*, concluiu-se que a utilidade percebida e a facilidade de uso da rede social estão relacionadas com a confiança e segurança do utilizador relativamente às mesmas.

Com os resultados de Ferreira (2014), foi possível retirar algumas conclusões em relação às redes sociais. Estas foram aplicadas no presente estudo, mas relativamente aos *Smartphones*, o que vai ao encontro do objetivo desta investigação, sendo o modelo de aceitação *TAM* um grande setor deste questionário e estudo. O modelo *TAM* é um dos três modelos incorporados no modelo *TUM*, que permite medir a aceitação da tecnologia com a combinação de três modelos diferentes.

Com os resultados sobre a questão (gráfico 29, *c.f.* apêndice A) da regularidade com que os estudantes utilizam o *Smartphone*, foi observado que 99,1% respondeu que

utiliza o seu *Smartphone* todos os dias e 0,9% respondeu que usa o *Smartphone* entre quatro a seis dias por semana. Com estes resultados, é fácil perceber que a maioria destes estudantes tem contacto diário com o *Smartphone*. Deste modo, é possível que o *Smartphone* registre dados sobre os utilizadores todos os dias, o que pode permitir uma grande base de dados de cada utilizador, logo, pode permitir a criação de um perfil mais exato de cada um. Também se observou mais um indicador forte de que a grande maioria dos estudantes, ao ter contacto diário com o *Smartphone*, é, de facto, *digitally savvy*.

Ao analisar os dados recolhidos relativamente ao tempo que os estudantes gastam, por dia, com este aparelho (gráfico 30, *c.f.* apêndice A), foi observado que a grande maioria de 60,6% indica, em média, estar mais de três horas por dia a utilizar o seu *Smartphone*. De seguida, verificou-se que 37,2% indicou gastar entre uma a duas horas, por dia, a utilizar o seu *Smartphone*, e, por fim, 2,2% indicou gastar menos de uma hora, por dia, com a utilização seu *Smartphone*. Estes resultados são importantes para ajudar a perceber a utilização que estes inquiridos fazem do *Smartphone*, assim como a quantidade de tempo que gastam com a utilização do mesmo.

Com a grande maioria dos inquiridos a indicar que gasta mais de três horas por dia com o *Smartphone*, pode-se perceber facilmente que este telemóvel desempenha um grande papel no dia-a-dia destes estudantes, que estes são *digitally savvy* e que o *Smartphone*, provavelmente, está presente em muitas situações e momentos privados dos inquiridos.

Saber há quantos anos os inquiridos têm um *Smartphone* é algo que ajuda a tirar conclusões importantes neste estudo. Observando o gráfico 31 (*c.f.* apêndice A), verificou-se que a grande maioria - 92,1% - indicou possuir um *Smartphone* há mais de três anos, entre um e três anos obteve-se 6,9% das respostas e 0,9% indicou possuir um *Smartphone* há menos de um ano. Concluiu-se que a grande maioria dos inquiridos, neste estudo, já tem bastante experiência com a utilização do *Smartphone*, tendo em conta que mais de três anos é um período longo.

A verificação do número de horas de utilização semanal dos estudantes também ajuda a perceber como é a utilização dos inquiridos (gráfico 32, *c.f.* apêndice A).

Os resultados desta questão, no gráfico 32, vieram confirmar as respostas dos estudantes na pergunta relativa ao número de horas que gastam diariamente com o

Smartphone. 57,1% dos estudantes indicou, pelo menos, utilizar o *Smartphone* 21 horas por semana, o que é relativamente coerente com os 60,6% que indicou (gráfico 30, c.f. apêndice A) usar o *Smartphone* mais de três horas por dia. Interessante também é a observação de que 6,3% dos estudantes indica utilizar o *Smartphone* mais de 50 horas por semana, o que significa um uso deste equipamento eletrônico superior a dois dias completos por semana. No entanto, a grande maioria de 54,6% indica usar o *Smartphone* entre 11 a 30 horas por semana.

4.2.9. Análise dos resultados relativamente à facilidade de uso percebida (FUP)

A facilidade de uso percebida é importante para analisar a aceitação da tecnologia, sendo uma componente do modelo *TAM* e o próximo setor do questionário, o grupo 6. As seguintes seis perguntas foram criadas com a base bibliográfica, de forma a ir ao encontro da facilidade de uso percebida.

Na análise dos dados recolhidos sobre o nível de esforço mental requerido pelos estudantes para a utilização do *Smartphone* (gráfico 34, c.f. apêndice A), 46,4% dos inquiridos respondeu que considera muito fácil aprender a utilizar o *Smartphone*, 44,5% considera bastante fácil, 6,9% considera uma facilidade neutra, 1,3% considera um pouco difícil e 0,9% considera que não é nada fácil aprender a utilizar o *Smartphone*. Verificou-se que a grande maioria dos inquiridos - 90,9% - respondeu que considera, pelo menos, bastante fácil aprender a utilizar o *Smartphone*. Isto permite concluir que, para a grande maioria dos utilizadores, aprender a utilizar um *Smartphone* não apresenta grandes obstáculos de aprendizagem. Pelo contrário, é considerado muito fácil, sendo, assim, um indicador para uma resistência inferior por parte dos utilizadores na aderência a esta tecnologia, o que ajuda a explicar a grande aderência aos *Smartphones*.

Na observação dos resultados obtidos e apresentados no gráfico 35 (c.f. apêndice A), verificou-se que a grande maioria de 69,4% dos inquiridos considera que a utilização do *Smartphone* requer pouco ou nenhum esforço mental. 19,6% indicou que não requer nenhum esforço mental, 49,8% considera que requer pouco esforço mental, 17% considera que requer um esforço mental neutro, 12,6% considera que requer algum esforço mental e 0,9% considera que a utilização do *Smartphone* requer muito esforço mental.

No gráfico 35 (*c.f.* apêndice A), procurou-se perceber se os estudantes consideram fácil comunicar com os seus contactos através do *Smartphone*. Observou-se uma grande maioria dos inquiridos a responder que considera muito fácil comunicar com os seus contactos através do *Smartphone* - 72,6%. Com a resposta de “bastante fácil” obteve-se 23,3%, para uma “facilidade neutra” obteve-se 3,8% e “pouco fácil” obteve apenas 0,3%. Assim, verificou-se que 95,9% dos inquiridos considera bastante ou muito fácil comunicar com os seus contactos através do *Smartphone*. Deste modo, foi possível concluir que o *Smartphone* é considerado, por estes inquiridos, uma ferramenta com uma facilidade percebida de comunicação boa.

De seguida, analisou-se a flexibilidade das ferramentas, de forma a poderem ser usadas da melhor maneira pelos estudantes.

Com a análise dos resultados obtidos e apresentados no gráfico 36 (*c.f.* apêndice A), verificou-se que as ferramentas são vistas, pela grande maioria dos estudantes, como flexíveis, de maneira a poderem usá-las da melhor forma. 93,7% respondeu com “sim” e apenas 6,3% respondeu com “não”. Isto serve também como indicador para a verificação, entre outros, de que estes estudantes têm os conhecimentos necessários para trabalhar corretamente com o *Smartphone* e de que são *digitally savvy*.

Os dados recolhidos sobre a consideração da facilidade da partilha de fotos, vídeos e estados no *Smartphone*, apresentados no gráfico 37 (*c.f.* apêndice A), mostraram que 60,9% dos inquiridos considera muito fácil, 33,1% considera bastante fácil, 5,7% considera uma facilidade neutra e 0,3% considera pouco fácil a partilha dos mesmos. Verificou-se que a grande maioria dos inquiridos tem uma boa facilidade percebida da partilha destes dados, considerando muito fácil a partilha dos respetivos itens da questão.

Na análise dos dados obtidos relativamente à flexibilidade da interação com o *Smartphone*, apresentada no gráfico 38 (*c.f.* apêndice A), verificou-se que 43,2% respondeu que era “muito flexível”, 44,2% respondeu que considerava “bastante flexível”, 11% respondeu que se tratava de uma “flexibilidade neutra” e 1,6% respondeu que era “pouco flexível”.

Verificou-se que a grande maioria dos inquiridos de 87,4% considera a interação com o *Smartphone*, pelo menos, bastante flexível. Assim, uma vez mais, é possível observar

indicadores de uma facilidade de uso percebida bastante positiva, na utilização do *Smartphone* pelos utilizadores.

4.2.10. Análise dos resultados relativamente à utilidade percebida (UP)

No presente setor do questionário, o grupo sete, analisou-se a utilidade percebida (UP), que é parte do modelo de aceitação *TAM*. As seguintes sete perguntas foram criadas a partir da revisão bibliográfica, de forma a responder a este objetivo.

Na pergunta apresentada no gráfico 39 (*c.f.* apêndice A), foi possível concluir que a grande maioria dos inquiridos - 72,6% - indica que considera muito útil, 23,3% indica que considera bastante útil, 3,2% indica que considera uma utilidade neutra, 0,6% indica que considera pouco útil e 0,3% indica que considera nada útil o uso do *Smartphone* para comunicar com a sua rede de contactos pessoais. Foi verificado que 95,9% dos inquiridos considera o *Smartphone*, pelo menos, bastante útil para a comunicação com a sua rede de contactos pessoal.

Com os dados recolhidos a partir da questão anterior (gráfico 40, *c.f.* apêndice A), verificou-se que a grande maioria de 53% respondeu que considera o uso do *Smartphone* muito útil para a comunicação com a sua rede de contactos universitários, 36,3% respondeu que era bastante útil, 8,5% respondeu que a utilidade era neutra, 1,9% respondeu que era com pouco útil e 0,3% respondeu que não era nada útil. Observou-se, então, que a grande maioria dos inquiridos - 89,3% - considera o *Smartphone*, pelo menos, bastante útil para comunicar com a sua rede de contactos universitários.

Com os dados obtidos relativamente à questão que procura saber a opinião dos estudantes no que diz respeito à utilidade de terem a possibilidade de partilhar fotos, vídeos e ficheiros pelo *Smartphone*, verificou-se o que consta no gráfico 41 (*c.f.* apêndice A). A grande maioria dos inquiridos - 52,1% - considera a possibilidade de partilhar fotos, vídeos e ficheiros pelo *Smartphone* muito útil, 37,2% considera bastante útil, 9,1% considera uma utilidade neutra, 1,3% considera pouco útil e 0,3% não considera nada útil. Assim, observa-se que 89,3% dos inquiridos indica que o *Smartphone* é, pelo menos, bastante útil para partilhar fotos, vídeos e ficheiros. Isto pode ser visto como um indicador de que o *Smartphone* é uma mais valia para estes fins, havendo uma utilidade percebida bastante positiva.

Na análise dos dados obtidos, através da questão relativa à rapidez do trabalho graças ao uso das ferramentas do *Smartphone*, apresentada no gráfico 42 (*c.f.* apêndice A), observou-se que a grande maioria (90,9%) indicou que o seu trabalho fica mais rápido ao usar o aparelho e apenas 9,1% indicou o contrário. Uma vez mais, observou-se que o *Smartphone* é visto como uma ferramenta útil em trabalho, uma razão para explicar o motivo de muitos estudantes (95,6%) terem indicado o seu uso para finalidades académicas, na questão 27 do presente estudo. É fácil de perceber que o uso do *Smartphone* é mais uma vantagem reconhecida pelos estudantes, no seu dia-a-dia, e que a quantidade de utilização do mesmo é justificada também por motivos relacionados com a produtividade dos universitários. É, claramente, mais um indício de que estes estudantes são *digitally savvy*.

Em relação ao aumento da eficácia dos estudantes ao utilizar o *Smartphone*, foi observado que 81,7% dos inquiridos respondeu que o seu uso, no trabalho diário, aumenta a sua eficácia, sendo que 18,3% indica que este não é o caso, como se apresentado no gráfico 43 (*c.f.* apêndice A).

Com os dados recolhidos sobre a questão que envolve o ponto de afetabilidade nos estudos devido ao uso do *Smartphone*, apresentados no gráfico 44, *c.f.* apêndice A, foi observada uma diversidade considerável entre as respostas dos estudantes. Estes dividem-se em dois grandes grupos, onde 38,2% indica sentir que o *Smartphone* afeta, pelo menos, bastante os estudos - 34,7% respondeu que afeta bastante e 3,5% respondeu que afeta muito - e 47% indicou que afeta pouco (42,9%) ou não afeta nada (4,1%) os seus estudos. Os restantes 14,8% responderam que não sente ter qualquer impacto nos seus estudos pelo *Smartphone*. Apesar de a grande maioria de 95,6% dos estudantes usar o *Smartphone* para uso académico, quase metade dos estudantes (47%) sente que este dispositivo afeta pouco ou nada os seus estudos.

Isto é um indicador que o *Smartphone*, dependendo de um certo uso, pode afetar muito os estudos, de alguma forma. No entanto, parece que muitos dos inquiridos não conseguem aperceber-se de tal possibilidade.

Na questão que se prende com a utilidade do *Smartphone* para os estudos destes universitários, representada no gráfico 45 *c.f.* apêndice A, é possível obter indicadores

sobre a utilidade percebida em relação ao usar o *Smartphone* nos estudos, mesmo antes de o utilizar para esse fim.

Com os dados recolhidos, verificou-se, como esperado, que 36,6% considerava uma utilidade neutra, o que faz sentido, visto que não utilizaram um *Smartphone* para esse fim e não conseguiram definir uma ideia mais específica. Mais de um terço dos estudantes (35%) indicou que considerava, já antes de possuir um *Smartphone*, que este seria bastante útil nos seus estudos - 8,8% até indicou que o considerava muito útil para esse fim. A percentagem que considera o *Smartphone* pouco e nada útil é de 13,9% e 5,7%, respetivamente.

4.2.11. Análise dos resultados relativamente à intenção comportamental (IC)

No próximo setor, que corresponde ao grupo 8 do questionário, analisou-se a intenção comportamental (IC). Esta faz parte do modelo *TAM* e as próximas oito perguntas do questionário foram elaboradas a partir da literatura para analisar exatamente esse aspeto.

Com a análise da intenção comportamental, é possível perceber certos aspetos direcionados para este trabalho. É importante perceber estas intenções relativamente aos *Smartphones*, de forma a poder avaliar e obter os resultados pretendidos. O modelo de aceitação da tecnologia *TAM* prevê a inclusão destes aspetos.

Perceber se estes estudantes pretendem usar o *Smartphone* sempre que possível pode mostrar o nível de aceitação desta tecnologia (gráfico 46, *c.f.* apêndice A). Aqui, 67,8% dos estudantes respondeu que “sim”. Verificou-se que este resultado é um indicador claro quanto ao nível de aceitação desta tecnologia, onde a grande maioria indica querer utilizar o *Smartphone* sempre que possível. Apenas 32,2% dos estudantes respondeu com um “não” a esta pergunta.

Na análise dos resultados obtidos, através da pergunta que procura saber se os estudantes têm intenção de aumentar o uso das ferramentas do *Smartphone*, apresentada no gráfico 47 (*c.f.* apêndice A), observou-se que 53,3% dos inquiridos tenciona aumentar esse uso e 46,7% indica que não tenciona fazê-lo. A maioria tenciona aumentar o uso das ferramentas, o que também significa que aceita utilizar o *Smartphone*, mesmo com os riscos de segurança envolvidos.

Com os dados recolhidos sobre a questão que pretende averiguar se os estudantes adorariam ter ferramentas novas no seu *Smartphone*, verificou-se que a grande maioria dos inquiridos, no futuro, adorava ter ferramentas novas no seu telemóvel, como representado no gráfico 48, *c.f.* apêndice A. Obteve-se um total de 81,1% a responder que sim e 18,9% a responder que não, o que pode ser um indicador de que a maioria dos inquiridos gosta e vê o *Smartphone* como uma ferramenta que pode ter ainda mais utilidade com a implementação de ferramentas novas.

Como mencionado ao longo deste estudo, a câmara é uma ferramenta crítica que está relacionada com um potencial risco elevado de revelar dados privados muito sensíveis. Tapar a câmara do *Smartphone* ou qualquer outro dispositivo com acesso à internet é um fenómeno que se observa muitas vezes, é algo que utilizadores fazem de forma a proteger a sua privacidade digital de terceiros.

Com a análise dos dados recolhidos sobre a necessidade de os estudantes taparem a câmara (gráfico 49, *c.f.* apêndice A), verificou-se que a grande maioria não tem necessidade de o fazer. No entanto, 29,3% dos estudantes sente essa necessidade. Isto mostra que estes estudantes (29,3%) teriam interesse em que o *Smartphone* tivesse alguma ferramenta ou funcionalidade que permitisse tapar e/ou desativar a câmara - uma implementação interessante seria a de um botão físico que permitisse desligar a câmara, interrompendo o circuito de energia. Este resultado também mostra a desconfiança que existe por este grupo de estudantes perante as organizações que tratam ou tem acesso aos dados do *Smartphone*.

Tendo em conta que o *GPS* possibilita a criação de perfis geográficos do utilizador, parece ser uma boa ideia desativar o mesmo quando não se está a utilizar. Na análise que procura saber se os estudantes desligam o *GPS* quando não o estão a usar, foi verificado (gráfico 50, *c.f.* apêndice A) que a grande maioria de 58,4% afirma desativar o *GPS* sempre que não precisa do mesmo e 41,6% afirma não desativar o *GPS*, mesmo que não precise do mesmo.

Na verificação dos resultados (gráfico 51, *c.f.* apêndice A) sobre a necessidade de desligar o *Smartphone* por completo durante os períodos que não o estão a usar, a grande maioria dos estudantes - 92,4% -, como esperado, não sente essa necessidade e apenas 7,6% indica que a sente. Este comportamento era previsível, visto que desligar o

Smartphone por completo não é “prático”, perde-se a possibilidade de ser contactado e, em necessidade espontânea de aceder a alguma funcionalidade do *Smartphone*, ter-se-ia de levar um tempo de resposta muito superior. Desligar o *Smartphone* por completo não parece ser a solução ideal e as desvantagens, ao que parece, não justificam esse comportamento, no ponto de vista dos inquiridos.

Na questão que remete para a intenção de adquirir uma aplicação para se defender da invasão de terceiros, representada no gráfico 52 *c.f.* apêndice A, foi verificado que a grande maioria de 59,3% indicou não ter intenções de adquirir uma aplicação para esse fim. A percentagem dos inquiridos que indicou ter intenções de o fazer é grande - 40,7%. Assim sendo, foi verificado que mais de metade dos inquiridos não parece estar preocupado com a possível invasão de terceiros ou, então, não acredita que uma aplicação para este fim seja eficaz. Estes resultados são semelhantes aos da pergunta 18, na qual se questionou a intenção de instalar uma aplicação já antes de ter um *Smartphone*, onde 54,3% indicou que considerava pouco ou nada necessário que tal se fizesse.

Procurou-se saber se os estudantes adoravam ter um botão que permitisse desligar o microfone do *Smartphone* para perceber se estes gostariam de ter mais opções que lhes possibilitasse um maior controlo próprio sobre os dados que este aparelho pode registar. Na análise dos dados obtidos e representados no gráfico 53, *c.f.* apêndice A, verificou-se que a grande maioria de 58% adorava ter um botão que permite esta funcionalidade e 42% não adorava ter um botão para este fim. A grande maioria tem o desejo de ter a opção de impedir o registo do microfone do *Smartphone*, de maneira prática e conveniente, como com um botão que permite essa funcionalidade.

4.2.12. Análise dos resultados relativamente ao uso real (UR)

No seguinte setor, que corresponde ao grupo 9, analisou-se o uso real (UR). Este é uma parte importante do modelo de aceitação *TAM* e as próximas cinco perguntas vão ao encontro de responder a questões do uso real dos inquiridos, relacionado com os objetivos deste estudo, no que diz respeito à privacidade de dados, na utilização do *Smartphone*.

Saber que aplicações predefinidas, neste estudo, são frequentemente utilizadas ajuda a verificar a preocupação dos inquiridos no que diz respeito à sua privacidade digital e

a uma possível recolha de dados privados por terceiros. Na análise dos resultados obtidos na questão 53, representada no gráfico 54, *c.f.* apêndice A, verificou-se que todas as funcionalidades apresentadas aos inquiridos são usadas, sendo apenas uma a que obteve uma percentagem inferior a 50%. As percentagens dividem-se da seguinte forma: Aplicação de mensagens - 95,9%; Aplicação de páginas web - 92,1%; Aplicação de e-mail - 87,7%; Aplicação da câmara - 86,1%; Aplicação de contactos - 85,8%, Aplicação do GPS - 75,7%; Aplicação do calendário - 60,6% e microfone - 48,9%.

De forma a perceber com que frequência os estudantes utilizam ferramentas do *Smartphone*, colocou-se a questão 54, representada no gráfico 55, *c.f.* apêndice A. Com a análise desta pergunta, verificou-se que a grande maioria de 86,4% indica usar as ferramentas do *Smartphone* todos os dias. Mais uma vez, verifica-se uma grande aderência por parte dos estudantes inquiridos, na utilização diária do *Smartphone*. 1,6% referiu que usava duas vezes por semana. A mesma percentagem de inquiridos revelou fazê-lo três vezes por semana. 3,2% indicou que a utilização era de quatro vezes por semana e 7,3% afirmou que o uso era de cinco ou seis vezes por semana.

Na análise dos dados recolhidos, de maneira a perceber se os estudantes costumam utilizar o *Smartphone* para partilhar dados e fotografias, apresentada no gráfico 56, *c.f.* apêndice A, verificou-se que a grande maioria de 93,7% dos inquiridos usa o *Smartphone* para esse fim e apenas 6,3% indica que não o costuma fazer. Este resultado vai ao encontro da questão número 40, onde 89,3% dos inquiridos considera o *Smartphone*, pelo menos, bastante útil para partilhar fotografias, vídeos e ficheiros.

Com a análise dos dados recolhidos, na pergunta 56 (gráfico 57, *c.f.* apêndice A) do questionário, sobre a utilização do *Smartphone* para monitorizar a atividade física e/ou desportiva, verificou-se que 56,8% dos estudantes indicou não usar o *Smartphone* para esse fim e 43,2% indicou que o fazia. Com estes dados, verificou-se que, para 43,2% dos inquiridos, o *Smartphone* também serve como uma ferramenta de assistência na atividade física. Este dispositivo oferece ferramentas de recolha e análise de dados, possibilitando a obtenção de conclusões sobre a atividade física dos inquiridos. Estes dados podem ser práticos para os utilizadores, mas também são muito úteis para a criação de perfis de utilizadores por parte das organizações. Estas, se acederem a estes dados, têm a possibilidade de avaliar a atividade e, eventualmente, o estado de saúde destes utilizadores. Estas informações podem ser muito benéficas para diversas

organizações - vender e usar estes dados para fins de marketing direcionado, por exemplo, pode significar a existência de riscos de segurança para os utilizadores.

Interessante também é perceber se os utilizadores, nas atividades físicas, utilizam o *GPS* para registar os dados de posicionamento. Os resultados estão representados no gráfico 58 *c.f.* apêndice A. Com os dados obtidos, verificou-se que 36,6% dos inquiridos costuma usar o *GPS* para as suas atividades físicas e a grande maioria de 63,4% indica que não costuma usar o *GPS* para este fim. Visto que, na pergunta 56, se verificou que 43,2% dos inquiridos utiliza o *Smartphone* para monitorizar as suas atividades físicas, a percentagem de 36,6% significa que a grande maioria dos inquiridos que utiliza o *Smartphone* para a monitorização física também ativa o *GPS*, nessas circunstâncias.

4.2.13. Análise dos resultados relativamente à confiança/segurança relacionada com a tecnologia

No último sector do questionário da recolha de dados deste estudo, que corresponde ao grupo 10, analisou-se a confiança/segurança no que diz respeito à tecnologia, neste caso, o *Smartphone*. As seguintes cinco perguntas vão atender a esse objetivo.

Na análise dos resultados que procura saber se os utilizadores divulgam as suas informações pessoais no *Smartphone*, apresentados no gráfico 59, *c.f.* apêndice A, verificou-se que a grande maioria o faz. 64% dos inquiridos respondeu que “sim” e 36% respondeu que “não” a esta pergunta. Com isto, verificou-se que 64% dos inquiridos confia estes dados ao seu *Smartphone*, o que pode corresponder a um certo nível de segurança percebida por parte de estes utilizadores, relativamente ao *Smartphone*.

Com a análise dos dados recolhidos no que diz respeito ao que pensam os estudantes relativamente ao *Smartphone* como um meio seguro para partilhar fotos, vídeos, ficheiros e informações pessoais, representada no gráfico 60, *c.f.* apêndice A, verificou-se que 47,6% dos inquiridos considera haver uma segurança neutra, 28,7% considera pouco seguro, 16,1% considera bastante seguro, 5% não considera nada seguro e 2,5% considera muito seguro usar o *Smartphone* com esta finalidade. Ao comparar estes resultados com os das perguntas 40 e 55, verificou-se que, apesar de 33,7% dos inquiridos considerar o *Smartphone* pouco ou nada seguro para partilhar estes dados, 93,7% costuma, mesmo assim, partilhá-los pelo *Smartphone*. Este comportamento

parece estar relacionado com o facto de 89,3% dos inquiridos considerar o *Smartphone*, pelo menos, bastante útil para partilhar estes dados.

De forma a avaliar se os inquiridos se sentem completamente seguros ao utilizar o *Smartphone* para comunicar com os seus contactos ou empresas, foi feita a questão número 60 do questionário, cujos resultados estão representados no gráfico 61, *c.f.* apêndice A. Na análise, verificou-se que estes variam bastante nas suas respostas - 43,5% dos inquiridos respondeu que sente uma segurança neutra, 33,8% indicou que se sente bastante seguro, 12,9% indicou que se sente pouco seguro, 7,9% indicou que se sente muito seguro e 1,9% indicou que não se sente nada seguro, ao utilizar o *Smartphone* para este tipo de comunicação.

Com a análise dos resultados obtidos relativamente à segurança percebida pelos estudantes, ao jogar as mais diversas aplicações no *Smartphone*, verificou-se um resultado muito semelhante ao da pergunta anterior. Com os resultados representados no gráfico 62, apêndice A, observou-se que 41,3% dos inquiridos indicou que sente uma segurança neutra, 29,3% indicou que se sente bastante seguro, 15,6% indicou que se sente muito seguro, 12,9% indicou que se sente pouco seguro e 1,3% indicou que não se sente nada seguro.

Com a análise da pergunta 62 (gráfico 63, *c.f.* apêndice A), que tem a finalidade de saber se os estudantes se sentem seguros ao utilizar o *Smartphone* para ter conversas privadas relacionadas com trabalho ou dados sensíveis, cujos resultados estão representados no gráfico 63, *c.f.* apêndice A, percebeu-se que o número de inquiridos se divide de forma equitativa entre pouco ou nada seguro e bastante ou muito seguro. 40,1% dos inquiridos respondeu que sente uma segurança neutra, 24,3% respondeu que se sentia bastante seguro, 21,1% respondeu que se sentia pouco seguro, 7,3% respondeu que não se sentia nada seguro e também 7,3% respondeu que se sentia muito seguro. Este resultado mostra que os estudantes estão proporcionalmente divididos na opinião sobre a segurança que sentem ao utilizar o *Smartphone* para este fim, o que explica a percentagem relativamente alta - 40,1% - que refere sentir uma segurança neutra.

No Apêndice C, estão representadas as conclusões das análises por questão de investigação, em detalhe, que foram desenvolvidas neste estudo.

Capítulo 5 – Conclusões e recomendações

5.1. Principais conclusões

Este trabalho contribui para o entendimento do fenómeno emergente da segurança de dados privados na utilização com *Smartphones*, onde têm surgido vários relatos sobre a utilização destes dados, sem a autorização e/ou conhecimento do utilizador. Este tipo de investigação é crescente devido à sua importância para sensibilizar as pessoas, no sentido de se criarem leis adicionais, com o intuito de proteger os cidadãos, na sua esfera da vida privada. De forma a perceber se os utilizadores de *Smartphones*, participantes neste estudo, têm conhecimento sobre o que acontece com os seus dados privados, recolhidos através do *Smartphone*, foram necessárias recolhas e análises de dados.

A revisão de literatura permitiu constatar que ainda não foram feitos estudos específicos, em Portugal, sobre a recolha de dados privados unicamente através do *Smartphone*. No entanto, existem vários estudos que se centraram na recolha de dados privados, através das redes sociais. Outra das conclusões retirada da revisão de literatura é facto de o crescimento de *Smartphones*, na população, continuar a crescer, sendo, cada vez mais, visto como uma ferramenta de uso para o dia a dia. Uma das conclusões mais importantes que surgiu no mesmo contexto é o facto de terceiros, com intenções maliciosas, poderem obter informações privadas sobre os utilizadores de *Smartphones*, através de aplicações instaladas no mesmo (Delac et al., 2011). Percebendo também que os estes aparelhos já têm funções semelhantes às de um computador normal, verifica-se uma grande possibilidade de recolha de dados privados de múltiplos tipos de aplicações, tais como, emails, navegador de internet, *GPS*, entre outros.

Na primeira fase da recolha de dados, realizou-se uma entrevista a 8 alunos para perceber a preocupação que estes têm com a proteção dos seus dados pessoais e se sabem os dados que as organizações de telecomunicações podem coletar sobre eles. Os resultados das entrevistas indicam que os utilizadores não têm comportamentos específicos, com o *Smartphone*, de forma a proteger a sua privacidade. Na maioria dos casos, estão à vontade com o *Smartphone* nas situações do dia a dia avaliadas neste estudo, sendo possível sugerir que, quanto mais à vontade se sentem, menos se protegem.

A segunda fase da recolha de dados realizou-se com a implementação de um questionário. Este foi disponibilizado aos alunos do primeiro ano de licenciatura dos cursos da escola ISTA do ISCTE-IUL. Os resultados indicaram que a maioria dos

estudantes inquiridos sabe que o uso do *Smartphone* tem riscos de segurança associados. A desconfiança dos inquiridos, perante as organizações de telecomunicações, foi um fator que se mediu neste estudo, tendo-se verificado que existe, claramente, uma certa desconfiança associada a estas organizações por parte da maioria dos inquiridos. Relativamente à segurança que os inquiridos sentem em relação à sua privacidade pessoal ao usar o *Smartphone*, observou-se que estes não se sentem muito seguros. No entanto, a insegurança não parece ser um fator determinante que leve a uma limitação do uso do *Smartphone*, de forma a proteger a sua privacidade com uma maior eficiência. Estes inquiridos parecem não estar particularmente insatisfeitos com o tratamento dos seus dados privados pelas organizações, embora também não estejam totalmente satisfeitos e apresentem incertezas sobre questões de confiança neste assunto. O *Smartphone* oferece mais ferramentas quando está conectado com a internet, tem o *GPS* ativo e acede ao microfone e à câmara. Os inquiridos fazem uso de todas estas ferramentas, tratando-se de um comportamento que comprova que os utilizadores permitem a criação de perfis mais completos pelas organizações. A maior parte dos inquiridos mostrou que sabe quais os dados que partilha com as organizações e que sabe que os mesmos são partilhados com terceiros. Ainda assim, observou-se que fazem uso do *Smartphone* e das suas ferramentas. No que toca aos dados privados introduzidos pelos inquiridos no *Smartphone*, observou-se que uma grande parte os introduz no aparelho. Em relação às vantagens que os *Smartphones* oferecem no dia-a-dia dos inquiridos, verificou-se que são vantagens significativas a vários níveis, como o aumento da eficácia no trabalho e na faculdade - a grande maioria indica mesmo que usa o *Smartphone* sempre que pode. Para muitos inquiridos, a dependência do *Smartphone* parece ser um fenómeno existente. Estes universitários disseram, na sua grande maioria, que fazem uma utilização do *Smartphone* todos dias e várias vezes ao longo dos mesmos, utilizando, principalmente, as suas ferramentas favoritas do telemóvel. Este estudo mostrou que a quantidade de uso do *Smartphone* é muito grande no dia-a-dia dos utilizadores. Com isto, verificou-se também que os utilizadores inquiridos são *digitally savvy*, pelo que têm um bom conhecimento relativamente à tecnologia e fazem um grande uso da mesma no seu dia-a-dia. As informações, que os utilizadores estudados fornecem às organizações que lhes disponibilizam os serviços, são muito variadas. A maioria dos utilizadores partilha e introduz dados privados, fotografias, ficheiros e tem conversas privadas com os seus contactos, através do *Smartphone*. Grande parte dos inquiridos sabe que estes dados estão a ser registados pelo *Smartphone* e pelas respetivas organizações que disponibilizam estes

serviços. Este trabalho permitiu concluir que estes inquiridos, apesar de desejarem uma maior proteção relativamente aos seus dados privados, não parecem estar muito preocupados com este facto. Indicaram, aliás, que vão continuar a utilizar o *Smartphone* sem grandes receios, ainda que não tenham essa proteção mais elevada. Foi verificado, neste estudo, que a utilização que os estudantes fazem dos seus dispositivos móveis é muito completa. A maioria deles utiliza todas as aplicações analisadas nesta investigação e utiliza o seu *Smartphone*, pelo menos, 21 horas por semana. Este número de horas semanais, por estudante, reflete que estes utilizam o *Smartphone* em várias atividades ligadas à sua vida privada, tais como os estudos, o trabalho, os contactos pessoais, as redes sociais, entre outras. Através dos resultados obtidos, verificou-se que a maioria dos estudantes prefere abdicar da sua privacidade digital perante terceiros, em função de conseguir fazer uso dos seus *Smartphones* e das suas aplicações gratuitas e convenientes em muitas situações. Assim, é possível concluir que a vida digital, no futuro, para mais de metade dos estudantes, pode ser analisada pelas empresas, sem que estas temam que os utilizadores tomem ações contra elas. Com isto, pode-se dizer que, futuramente, a maioria dos utilizadores está disposta a ter uma vida digital transparente, pelo menos perante as organizações que lhes facultam os serviços.

5.2. Contributos para a comunidade científica e empresarial

5.2.1. Implicações ao nível académico

Do ponto de vista académico, o presente estudo mostrou que o *Smartphone* é utilizado pela grande maioria dos estudantes (95,1%) para uso académico, como observado no gráfico 27. O *Smartphone* também é considerado por 52,4% dos estudantes inquiridos como muito útil para comunicar com a rede de contactos universitários, havendo 37,2% que considera o *Smartphone* bastante útil para este mesmo fim, como se pode observar no gráfico 39. Este aparelho, com as suas ferramentas, segundo 90,9% dos estudantes inquiridos, aumenta a rapidez no seu trabalho - gráfico 41. No que toca à eficiência no trabalho 81,4%, também foi referido que esta aumenta com a utilização do *Smartphone*.

O aumento da produtividade é uma vantagem muito grande para qualquer pessoa, tanto a nível de trabalho, como de faculdade. Com o peso da carga de horário e da matéria escolar, o aumento da eficiência e da produtividade pode significar a diferença entre obter bons ou maus resultados.

Depois da análise dos dados deste estudo, o *Smartphone* já parece ter uma utilidade significativa para os estudantes, ao nível académico. Isto pode ser um indicador no que diz respeito à presença de oportunidades neste nível, onde a implementação de ferramentas disponibilizadas pela faculdade, através do *Smartphone*, pode significar um benefício para a instituição e para os estudantes.

5.2.2. Implicações ao nível empresarial

Os resultados do presente estudo podem trazer conclusões vantajosas a nível empresarial, mais especificamente a nível da aceitação da tecnologia, onde foi feito o primeiro estudo com o modelo de aceitação *TUM*, em Portugal, principalmente em no que diz respeito à tecnologia relacionada com a privacidade de dados com o uso de *Smartphones* - o foco deste estudo.

Visto que os participantes do estudo representam as gerações jovens da população, na qual se têm os *Digital Natives* – cujos anos de nascimento se situam no intervalo entre 1991 e 2000 -, e a *iGeneration* – cujos anos de nascimento se iniciam a partir do ano 2000. Estas gerações representam o futuro da população adulta. Trata-se da população mais jovem no mercado de trabalho e parece evidente a sua importância ao nível empresarial, sendo relevante estudar esta população com o propósito de otimizar a performance de negócio, no presente e num futuro próximo, a nível da aceitação da tecnologia relacionada com o tratamento dos dados de privacidade dos estudantes.

É possível tirar várias conclusões valiosas deste estudo a nível empresarial, tal como o facto de 95,1% dos estudantes indicar que utiliza o *Smartphone* para fins académicos, o que se observa no gráfico 27. No entanto, o foco remete para as conclusões que vão ao encontro do objetivo deste estudo, isto é, saber o que os utilizadores aceitam ou não em relação ao tratamento dos seus dados privados e quais os riscos envolvidos.

Uma das conclusões é o facto de 96,6% dos inquiridos responder que continuaria a utilizar o *Smartphone*, mesmo tendo conhecimento dos riscos de segurança envolvidos, o que certamente é agradável para as empresas envolvidas neste ramo de negócio – gráfico 26. No entanto, observou-se que existe uma certa desconfiança e preocupação, por parte da grande maioria dos utilizadores, relacionadas com a proteção da sua privacidade no uso dos *Smartphones*. Previamente à aquisição de um *Smartphone*, 91,2% dos inquiridos indicou, pelo menos, considerar a existência de poucos riscos de privacidade, relativamente aos dados privados, como se pode observar no gráfico 16. 78% dos utilizadores também indicou já ter tido momentos nos quais se preocupou com a sua privacidade, ao utilizar o *Smartphone*, o que se pode observar no gráfico 19. 58,5% indicou que adoravam ter um botão que desligasse o microfone do *Smartphone*, como se pode observar no gráfico 52. 29,3% indicou já ter tido a necessidade de tapar a câmara do *Smartphone* em certas circunstâncias, o que se pode observar no gráfico 48. Atendendo

aos resultados apresentados neste estudo, as empresas podem ganhar uma vantagem competitiva, ao permitir um maior controlo sobre as ferramentas base dos telemóveis.

5.3. Limitações e dificuldades do estudo

Como esperado, esta investigação tem limitações, as quais estão relacionadas com o método aplicado para a recolha de dados, com a população escolhida e com o tema da dissertação em si.

Os métodos aplicados nesta investigação foram os de entrevista e questionário. O método de questionário tem as suas vantagens, as quais fizeram com que fosse o método escolhido para esta investigação. No entanto, as suas limitações são evidentes. Estas limitações têm de se levar em consideração na presente investigação. Visto que o questionário de resposta fechada não permite que os participantes, no estudo, tragam nada de novo ao mesmo, isto faz com que seja possível obter apenas resultados restritos. As perguntas, neste questionário, foram fundamentadas através da análise da revisão de literatura.

A escolha da população, neste estudo, também é uma limitação. Trata-se de uma população específica de alunos universitários do primeiro ano de licenciatura. Devido ao tempo e aos recursos limitados numa investigação de mestrado, não seria viável fazer uma investigação a nível nacional e com uma amostra de milhares de participantes. Isto faz com que este estudo seja apenas representativo para um grupo específico de participantes. No entanto, é o grupo ideal para representar as gerações *Digital Natives* (1991 - 2000) e *i Generation* (>2000), que representam o grupo mais novo de população adulta atual, tratando-se de estudantes da escola ISTA do ISCTE. Estes jovens adultos são as gerações que, futuramente, terão o poder de mudança, e aos quais a indústria se deve adaptar para ter resultados satisfatórios, tanto no ramo da privacidade de dados destes adultos, como na disponibilização de serviços através dos *Smartphones*.

A escolha do tema da dissertação em si está relacionada com a falta de estudos e de bibliografia científica, devido à rápida evolução e alteração que dificultam a permanente atualização do conhecimento na área em estudo. Por vezes, não se conseguiu encontrar bibliografia relacionada com temas que se queria ter implementado na dissertação. Este campo de estudo tem muito a ver com a evolução das tecnologias móveis, a qual sofre constantes alterações ao longo do tempo, devido, entre outros, a novas leis, às políticas de privacidade das empresas e da dependência da utilização dos dispositivos móveis.

5.4. Recomendações para investigações futuras

Considerando o estudo efetuado, sugere-se para investigações futuras:

- Aplicar este instrumento de investigação a um grupo maior de estudantes universitários, englobando mais institutos superiores e as universidades em todo país, por exemplo. Seria possível verificar a existência de resultados estatisticamente diferentes, em diversas regiões do país. Poder-se-iam comparar grupos regionais distintos, de forma a verificar se a experiência e a percepção de segurança destes utilizadores de *Smartphone* eram muito distintas, tais como a uma população mais velha, por volta dos 40 anos.
- Investigar até que ponto é possível que as instituições de telecomunicações usem os dados privados dos utilizadores, sem serem detetadas por ninguém. Poder-se-ia averiguar se estes usam determinados métodos, de maneira a poderem fugir às leis, e que promessas fazem relacionadas com a proteção dos dados privados dos utilizadores.
- Desenvolver um guião de recomendações sobre o uso do *Smartphone*, com o propósito de minimizar os dados privados recolhidos dos utilizadores e perceber se os utilizadores aceitariam esse guião, principalmente se confrontados com os riscos envolvidos.

Bibliografia

- ANACOM. (2017). Banda larga móvel com 6,6 milhões de utilizadores - Destaques - Portal do Consumidor. Retrieved November 12, 2018, from <http://www.anacom-consumidor.com/-/banda-larga-movel-com-6-6-milhoes-de-utilizadores>
- ANACOM. (2020). Tráfego de banda larga móvel aumenta 36,8% em 2019. Retrieved July 21, 2020, from <https://www.anacom.pt/render.jsp?contentId=1512981>
- Anshari, M., & Alas, Y. (2015). Smartphones habits, necessities, and big data challenges. *Journal of High Technology Management Research*, 26(2), 177–185. <https://doi.org/10.1016/j.hitech.2015.09.005>
- Arxan. (2016). *January 2016 L 5th Annual State of Application Security Report Perception vs. Reality Financial Services Edition*. Retrieved from https://www.csa.limited/State_of_Application_Security_2016_FinServ_Report.pdf
- Au, Y. A., & Kauffman, R. J. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic Commerce Research and Applications*, 7(2), 141–164. <https://doi.org/10.1016/J.ELERAP.2006.12.004>
- Bell, Alexander G. (1876). Experimental Telephone. Retrieved July 27, 2020, from https://www.si.edu/object/alexander-graham-bell-experimental-telephone:nmah_689864
- Bell, J. (1993). *Doing Your Research Project: A Guide for First-time Researchers in Education and Social Science*. (U. of California, Ed.) (Open Unive). Open University Press, 1993.
- Bell, J. (1997). *Como realizar um projecto de investigação : um guia para a pesquisa em ciências sociais e da educação*. Gradiva. Retrieved from <https://repositorioaberto.uab.pt/handle/10400.2/8169>
- Boni, V., & Quaresma, J. (2005). Aprendendo a entrevistar : como fazer entrevistas em Ciências Sociais. *Revista Eletronica Dos Pós Graduados Em Sociologia Política Da UFSC*, 2(3), 68–80. <https://doi.org/10.5007/%X>
- Cardozo, R., McLaughlin, K., Harmon, B., Reynolds, P., & Miller. (1993). Product-market choices and growth of new businesses. *The Journal of Product Innovation Management*, 10(4), 331–340. [https://doi.org/10.1016/0737-6782\(93\)90075-2](https://doi.org/10.1016/0737-6782(93)90075-2)

- Carey, N. (2011). *Examining the security approaches employed in Apple's iOS and Google's Android*.
- Check Point. (2017). *A CISO's Guide to Mobile Threat Prevention*.
- Cibersegurança, C. N. (2020). Boas práticas » Recursos » Centro Nacional de Cibersegurança. Retrieved July 21, 2020, from <https://www.cncs.gov.pt/recursos/boas-praticas/>
- Conceito.de. (2011). O que é, Definição e Significado de Segurança. Retrieved July 21, 2020, from <https://conceito.de/seguranca>
- Conceito.de. (2013). Conceito de privado - O que é, Definição e Significado. Retrieved July 21, 2020, from <https://conceito.de/privado>
- David J. Sheskin. (2004). *Handbook of Parametric and Nonparametric Statistical Procedures* (Third Edit). Boca Raton. Retrieved from file:///C:/Users/bruno/Downloads/9780429186165_googlepreview.pdf
- Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 319. <https://doi.org/10.2307/249008>
- Delac, G., Silic, M., & Krolo, J. (2011). Emerging security threats for mobile platforms. *MIPRO 2011 - 34th International Convention on Information and Communication Technology, Electronics and Microelectronics - Proceedings*, 1468–1473.
- Deshpande, S., & Dharmadhikari, S. C. (2016). *Analysis on Camera Attacks and their Defenses on Android Smartphones*. *European Journal of Advances in Engineering and Technology* (Vol. 3). Retrieved from <http://www.ejaet.com/PDF/3-3/EJAET-3-3-26-29.pdf>
- Domingos Silva Júnior, S. DA, & José Costa, F. DA. (2014). XVII SEMEAD Seminários em Administração Mensuração e Escalas de Verificação: uma Análise Comparativa das Escalas de Likert e Phrase Completion.
- Dwyer, C., Roxanne Hiltz, S., Passerini, K., & Roxanne, S. (2007). *Association for Information Systems AIS Electronic Library (AISeL) Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace* Recommended Citation "Trust and Privacy Concern Within Social Networking Sites: A Comparison" (Vol. 339). Retrieved from

- <http://aisel.aisnet.org/amcis2007/339Dwyeret.al>.
- Edwards, J. (2018). Harry Helson's Adaptation-Level Theory, Happiness Treadmills, and Behavioral Economics. *Journal of the History of Economic Thought* (Cambridge University Press), 40(1), 1–22.
- Fazal-e-Amin. (2015). Characterization of web browser usage on smartphones. *Computers in Human Behavior*, 51, 896–902.
<https://doi.org/10.1016/J.CHB.2014.10.054>
- Ferreira, D. B. de S. (2014). *A influência do modelo de aceitação da tecnologia na utilização da rede social Facebook na perspectiva do perfil pessoal*. Retrieved from http://recipp.ipp.pt/bitstream/10400.22/5057/1/DM_Daniela_Ferreira_2014.pdf
- Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. *Statistics* (Vol. 58). Retrieved from [https://books.google.pt/books?hl=pt-PT&lr=&id=c0Wk9IuBmAoC&oi=fnd&pg=PP2&dq=Field,+A.+\(2013\).+Discovering+Statistics+with+IBM+SPSS+Newbury+Park,+CA:+Sage&ots=LbHiHNXuZI&sig=ZRJ5ueD8E1WgTLbB1ORoAqi-sto&redir_esc=y#v=onepage&q=Field%2C+A.\(2013\).Discoverin](https://books.google.pt/books?hl=pt-PT&lr=&id=c0Wk9IuBmAoC&oi=fnd&pg=PP2&dq=Field,+A.+(2013).+Discovering+Statistics+with+IBM+SPSS+Newbury+Park,+CA:+Sage&ots=LbHiHNXuZI&sig=ZRJ5ueD8E1WgTLbB1ORoAqi-sto&redir_esc=y#v=onepage&q=Field%2C+A.(2013).Discoverin)
- Frambach, R. T., & Schillewaert, N. (2002, February 1). Organizational innovation adoption: A multi-level framework of determinants and opportunities for future research. *Journal of Business Research*. Elsevier. [https://doi.org/10.1016/S0148-2963\(00\)00152-1](https://doi.org/10.1016/S0148-2963(00)00152-1)
- Galloway, S., & Sean Keach, D. T. and S. E. (2016). Apple iPhone sales by year 2007-2016 | Statista. Retrieved December 15, 2018, from <https://www.statista.com/statistics/276306/global-apple-iphone-sales-since-fiscal-year-2007/>
- Ghisi, S., & Pezzella, M. C. C. (2014). PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO E O DIREITO À “INVISIBILIDADE” NOS ESPAÇOS PÚBLICOS. *Unoesc International Legal Seminar*, 0(0), 243–262.
- Gil, A. C. (2008). *Métodos e Técnicas de Pesquisa Social (Sexta Edição)*. Atlas S.A. Retrieved from <https://ayanrafael.files.wordpress.com/2011/08/gil-a-c-mc3a9todos-e-tc3a9cnicas-de-pesquisa-social.pdf>
- Hair Jr., J., Anderson, R. E., Tatham, R. L., Black, W. C., Sant'Anna, A. S., Chaves

- Neto, A., & Gouvêa, M. A. (2006). *Análise multivariada de dados*. Bookman.
- Hill, D. (2018). Expert Reference Series of White Papers Smartphones Explained Smartphones Explained, 1–11. Retrieved from www.globalknowledge.com
- Hill, R. J., Fishbein, M., & Ajzen, I. (1977). Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. *Contemporary Sociology*, 6(2), 244. <https://doi.org/10.2307/2065853>
- Huang, E. Y., & Lin, S.-W. (2014). How does e-mail use affect perceived control of time? *Information & Management*, 51(6), 679–687. <https://doi.org/10.1016/J.IM.2014.05.013>
- Hund, P. M., Dowell, J., & Mueller, K. (2014). Representation of time in digital calendars: An argument for a unified, continuous and multi-granular calendar view. *International Journal of Human-Computer Studies*, 72(1), 1–11. <https://doi.org/10.1016/J.IJHCS.2013.09.005>
- Kim, C., Shin, D., Shin, D., & Zhang, X. (2011). Improved Steganographic Embedding Exploiting Modification Direction in Multimedia Communications (pp. 130–138). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-22339-6_16
- Landis, J. R., & Koch, G. G. (1977). The Measurement of Observer Agreement for Categorical Data. *Biometrics*, 33(1), 159. <https://doi.org/10.2307/2529310>
- Leffler, A., & Roloff, M. E. (2006). Interpersonal Communication: The Social Exchange Approach. *Contemporary Sociology*, 11(6), 718. <https://doi.org/10.2307/2068564>
- Lell, J., & Nohl, K. (2018). *Uncovering the Android Patch Gap Through Binary-Only Patch Level Analysis*. *HIBTSecConf*. Retrieved from <https://conference.hitb.org/hitbsecconf2018ams/materials/D2T1 - Karsten Nohl & Jakob Lell - Uncovering the Android Patch Gap Through Binary-Only Patch Level Analysis.pdf>
- Levin, D. T., Harriott, C., Paul, N. A., Zhang, T., & Adams, J. A. (2013). Cognitive Dissonance as a Measure of Reactions to Human-Robot Interaction. *Journal of Human-Robot Interaction*, 2(3), 1–17. <https://doi.org/10.5898/JHRI.2.3.Levin>
- Lim, A. S. (2008). Inter-consortia battles in mobile payments standardisation. *Electronic Commerce Research and Applications*, 7(2), 202–213.

<https://doi.org/10.1016/J.ELERAP.2007.05.003>

Marcos, S., De, R., Aldemar, C., & Castro, A. (n.d.). *PROJETO DE PESQUISA (PARTE VIII-MÉTODO ESTATÍSTICO / TAMANHO DA AMOSTRA) Informações gerais 2. Projeto de pesquisa 2.1. Razões e objetivos da pesquisa 2.1.1. Contexto (justificativa) 2.1.2. Hipótese 2.1.3. Objetivo 2.2. Plano de trabalho e métodos- Comitê* . Retrieved from <http://www.evidencias.com/planejamento><http://www.metodologia.org><http://www.evidencias.com/planejamento><http://www.metodologia.org>

Mark L. Berenson, D. M. L. (1996). *Basic Business Statistics and Surfing for Success Business Student Guide to Internet Package: Amazon.in: Mark L. Berenson, David M. Levine: Books*. Pearson; 6 edition (8 May 1996). Retrieved from https://www.amazon.in/Business-Statistics-Surfing-Success-Internet/dp/0135780551/ref=sr_1_8?qid=1579105103&refinements=p_27%3AMark+L.+Berenson&s=books&sr=1-8

Martyn Denscombe. (2001). *The Good Research Guide: For Small-Scale Social Research Projects: for small-scale social research projects*. Open University Press.

McDaniel, C. J., & Gates, R. (2004). *Marketing Research Essentials. Marketing Research Essentials, 4th Edition*. Retrieved from https://trove.nla.gov.au/work/7264599?q&sort=holdings+desc&_=1570815927873&versionId=28947902

Meng, W., Wang, Y., Wong, D. S., Wen, S., & Xiang, Y. (2018). TouchWB: Touch behavioral user authentication based on web browsing on smartphones. *Journal of Network and Computer Applications, 117*, 1–9. <https://doi.org/10.1016/J.JNCA.2018.05.010>

Messias, I. (2017). *Ambientes híbridos em educação a distância : cenários para a criação de envolvimento do estudante na rede*. Retrieved from <https://repositorioaberto.uab.pt/handle/10400.2/6630>

Morettin, P. A., & Bussab, W. o. (2017). *Estatística Básica*. Saraiva.

Morvan, C., & O'Connor, A. J. (2017). *A theory of cognitive dissonance. A Theory of Cognitive Dissonance*. Stanford, California: Row, Peterson and Company.

- <https://doi.org/10.4324/9781912282432>
- Obar, J. A., & Oeldorf-Hirsch, A. (2018). *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*. Retrieved from <https://ssrn.com/abstract=2757465>
- Pinpathomrat, N. (2015). Technology usage model (TUM). In *Proceedings 2015 International Conference on Science and Technology, TICST 2015* (pp. 366–370). IEEE. <https://doi.org/10.1109/TICST.2015.7369387>
- Rosen, L. D., Carrier, M. L., & Cheever, N. A. (2010). *Rewired: understanding the iGeneration and the way they learn*. Palgrave Macmillan.
- Rothacher, M., & Beutler, G. (1998). The role of GPS in the study of global change. *Physics and Chemistry of the Earth*, 23(9–10), 1029–1040. [https://doi.org/10.1016/S0079-1946\(98\)00143-8](https://doi.org/10.1016/S0079-1946(98)00143-8)
- Rudas, T. (2011). *Odds Ratios in the Analysis of Contingency Tables. Odds Ratios in the Analysis of Contingency Tables*. <https://doi.org/10.4135/9781412985338>
- Sharma, S. (1996). *Applied multivariate techniques*. J. Wiley.
- Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers*, 22(5), 428–438. <https://doi.org/10.1016/j.intcom.2010.05.001>
- Slawik, M., Zilci, B. Ā., & Küpper, A. (2018). Establishing User-centric Cloud Service Registries. *Future Generation Computer Systems*, 87, 846–867. <https://doi.org/10.1016/J.FUTURE.2018.03.010>
- Snowden, E. (2019). *Permanent Record*. (Pan MacMillan, Ed.). Retrieved from <https://www.wook.pt/livro/permanent-record-edward-snowden/23232984>
- Suleiman, D., & Al-Naymat, G. (2017). SMS Spam Detection using H2O Framework. *Procedia Computer Science*, 113, 154–161. <https://doi.org/10.1016/J.PROCS.2017.08.335>
- Ter Louw, M., Lim, J. S., & Venkatakrishnan, V. N. (2008). Enhancing web browser security against malware extensions. *Journal in Computer Virology*, 4(3), 179–195. <https://doi.org/10.1007/s11416-007-0078-5>
- Tuckman, B. W. (2000). *Manual de investigacao em educacao: como conceber e*

- realizar o processo de investigacao em educaçao*. (F. C. Gulbenkian, Ed.), *Fundação Calouste Gulbenkian*. Retrieved from <https://www.bertrand.pt/livro/manual-de-investigacao-em-educacao-bruce-w-tuckman/76469>
- Vallina-Rodriguez, N., & Sundaresan, S. (2017). 7 in 10 Smartphone Apps Share Your Data with Third-Party Services | Knowridge Science Report. *Knowridge Science Report*. Retrieved from <https://knowridge.com/2017/06/7-in-10-smartphone-apps-share-your-data-with-third-party-services/>
- Waheed, A., & Khan, M. (2010). Attacks against Smartphones. *Citeseer*. Retrieved from <https://pdfs.semanticscholar.org/73e7/b25b355a9880c2111cf87b56931a3c2e2f3a.pdf>
- Wang, J. L., & Loui, M. C. (2009). Privacy and ethical issues in location-based tracking systems. In *International Symposium on Technology and Society, Proceedings* (pp. 1–4). IEEE. <https://doi.org/10.1109/ISTAS.2009.5155910>
- Warren, S. D., & Brandeis, L. D. (1890). *The Right to Privacy*. *Harvard Law Review* (Vol. 4). Retrieved from <https://www.jstor.org/stable/1321160>
- Xiong, J., & Jamieson, K. (2013). SecureArray. In *Proceedings of the 19th annual international conference on Mobile computing & networking - MobiCom '13* (p. 441). New York, New York, USA: ACM Press. <https://doi.org/10.1145/2500423.2500444>
- Yuan, M. J. (2005). What Is a Smartphone, 1–4. <https://doi.org/10.1103/PhysRevB.71.235415>
- Zhaw. (2014). Smartphones are becoming increasingly important to young people. *JAMES Study*, (October), 17–35. Retrieved from www.psychologie.zhaw.ch

Anexos e Apêndices

Anexo A – Exemplos de fuga de dados privados

Caso 1:

Segue um caso, que veio a público, onde ocorreu uma fuga⁴ de dados de utilizadores para terceiros (desconhecidos), através dos serviços da Google, que também são utilizados com os *Smartphones*. A Google reagiu e comunicou publicamente o problema e as precauções que tomou para impedir este tipo de fugas no futuro.

Google is shutting down its beleaguered social network sooner than expected in the wake of a new security issue that affected 52.5 million users.

Google Plus received its initial kiss of death in early October, when the company revealed that a security bug had exposed the account information of 500,000 users, including their names, email addresses and occupations. At the time, Google planned to shut down the social network by August 2019.

But in a blog post Monday Google wrote that it discovered a second bug that allowed the profile information of 52.5 million users to be viewable by developers, even if the profiles were set to private, using one of Google's application programming interfaces, or APIs, for six days in November. Once again, the available data included information like users' names, email addresses, occupations and ages.

Google said that the bug did not give third-party apps access to users' financial data or passwords and that it didn't find any evidence that the private profile information was accessed or misused. However, it now plans to shut down Google Plus by April 2019, and access to its APIs in the next 90 days.

*Google's initial security bug raised hackles in Washington and with the general public because *The Wall Street Journal* reported at the time that Google didn't disclose it for months because it feared regulatory scrutiny and reputational damage.*

Monday's disclosure comes a day before Google CEO Sundar Pichai is set to testify before Congress about transparency and accountability.

⁴ <https://www.cnbc.com/2018/12/10/google-shutting-down-social-network-sooner-because-of-new-security-bug.html>

“We understand that our ability to build reliable products that protect your data drives user trust,” Google’s blog post said.

“We have always taken this seriously, and we continue to invest in our privacy programs to refine internal privacy review processes, create powerful data controls, and engage with users, researchers, and policymakers to get their feedback and improve our programs.”

The enterprise version of Google Plus will remain active.

Caso 2:

Num outro caso que também veio a público, os utilizadores de iPhones⁵ podiam, sem saber, transmitir áudios e vídeos do seu dispositivo, através da aplicação *Facetime*, da Apple, devido a um erro de programação.

It was a tin-foil hatted conspiracy theorist's wildest prognostication come true: the trusty and beloved iPhones that accompany users to work, to bed and even to the toilet suddenly transformed into an all-purpose spying device, transmitting audio and video to anyone with your phone number or email.

"This is the nightmare scenario," said Marcus Carey, a cybersecurity expert and author of Tribe of Hackers. "It does incite privacy fears because this is the same scenario that most people fear from the US government and other regimes."

The bug, which was publicized Monday, transmitted audio (and, under certain circumstances, video) to a caller despite the recipient not having accepted the call. It was triggered when the initial caller added a third person to a FaceTime call. Though Apple has yet to issue a software patch, the company has disabled group chatting on FaceTime, preventing users from further exploiting the bug.

Advertisement

But the major flaw in FaceTime has raised concerns about Apple's security practices just as the company reports disappointing financial results. And reports that a teenager and his mother spent days attempting to alert Apple to the problem have also raised questions about the company's procedures for receiving reports of vulnerabilities.

Michele Thompson, an Arizona attorney whose identity was confirmed by the Wall Street Journal, began posting about her son's discovery of the bug on Facebook and Twitter on 20 January – eight days before Apple took action.

⁵ <https://www.theguardian.com/technology/2019/jan/29/facetime-security-bug-apple-privacy-iphone>

“My son just found a major flaw in Apple’s new iOS, that allows you to hear another person in the vicinity of their iPhone or iPad,” Thompson wrote on Facebook. “We just submitted the bug report to Apple and are waiting to hear back. We won’t provide the details since it’s a major security risk, but it’s unbelievable that my 14-year-old figured this out.”

Thompson made numerous attempts to alert Apple to the problem, first through social media and later through the company’s customer service system, according to the Journal. She eventually went so far as to register as a developer in order to submit a report through Apple’s bug bounty program.

Katie Moussouris, the founder of Microsoft’s bug bounty program and CEO of Luta Security, said that the problem for Apple was not that it failed to act quickly enough to patch the bug, but that it failed to manage Thompson’s expectations of how quickly a bug can be patched.

Apple rushes to fix FaceTime bug that let users eavesdrop on others

“It’s best not to rush,” Moussouris said. “You have to do in-depth investigations or else you can have unintended consequences. You don’t want people issuing patches that no one trusts or that break other things.”

For Apple, the best case scenario would have been to keep the existence of the vulnerability secret until the patch was tested and ready, Moussouris explained, a process that could reasonably take 30 to 60 days.

“You have to do this balance between thoroughness and timing, and in this circumstance there were misunderstandings that are understandable, and a missed opportunity for level-setting expectations,” she said.

That a phone call should start transmitting audio before the recipient picks up is counterintuitive to the lay person, but FaceTime was probably designed that way on purpose, according to someone who has built a similar system.

Luke Ma, the director of product management at video conferencing company BlueJeans Network, explained that software like FaceTime will initiate audio and video connections as soon as the call is made, and then mute them until the call is accepted.

“In order to accelerate speed of connection, your call is fully connected as soon as it can and your ‘answering’ the call basically just un-mutes everything,” Ma said.

Or, as Dr Jonathan Hill, dean of computer science and information systems at Pace University, put it, the ability for your phone to send audio before you answer is “not a bug. It’s a feature.”

The bug itself was likely a “logic error”, said Dr Lukasz Olejnik, an independent cybersecurity and privacy researcher.

“Logic errors make systems behave in unexpected ways,” he explained, and may just be the result of oversight. “Apple has one of the best security and privacy teams in the world. This case highlights how difficult proper security and privacy can be in practice.”

Carey said that the FaceTime bug was “a black eye” for a company that does indeed have a strong reputation for security and privacy.

“They’re going to have to be fully transparent on how this bug happened, and when it was introduced,” Carey said. “They need to release information about whether they can track to see if it was exploited, and they should notify customers.”

Apple did not respond to numerous queries from the Guardian requesting additional information about the bug.

Apêndice A – Gráficos da análise de dados

Resultados dos questionários aplicados aos estudantes

4. Maioritariamente utiliza a Internet no seu Smartphone para:

317 respostas

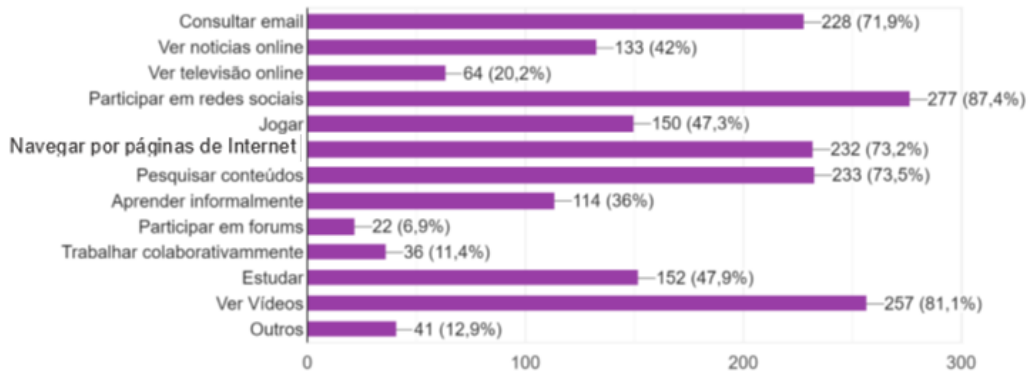


Gráfico 5 – Utilização da internet com Smartphone

5. Há quantos anos tem Smartphone pessoal?

317 respostas

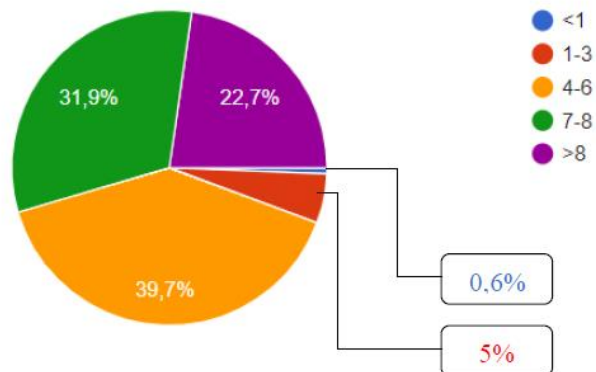


Gráfico 6 – Anos com Smartphone pessoal

6. Indique como se liga à Internet com o Smartphone:

317 respostas

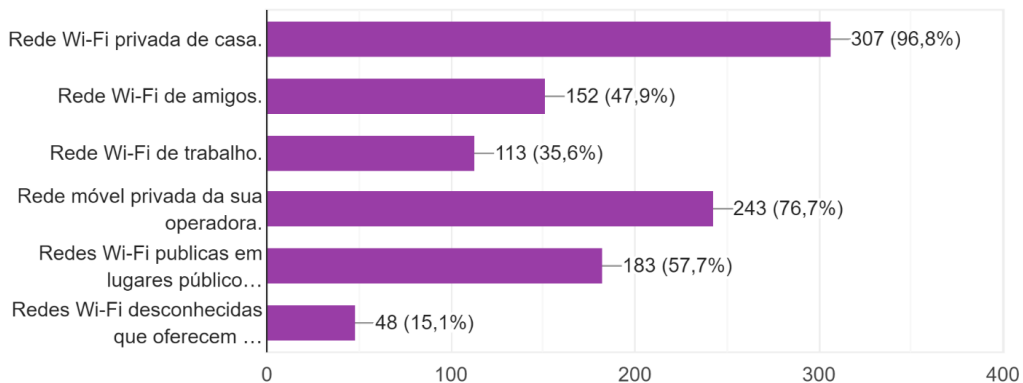


Gráfico 7 – Como inquiridos se ligam à internet

7. Indique quais destas aplicações usa no seu Smartphone?

317 respostas

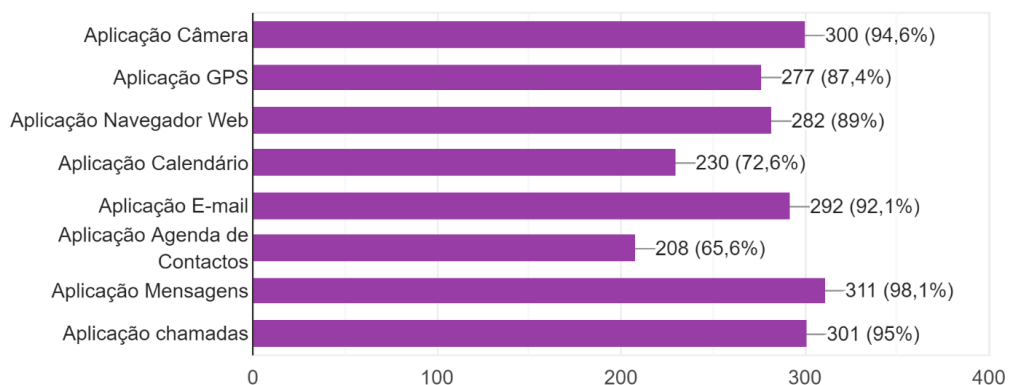


Gráfico 8 – Aplicações usadas no Smartphone

8. Com que frequência está online na sua aplicação preferida?

317 respostas

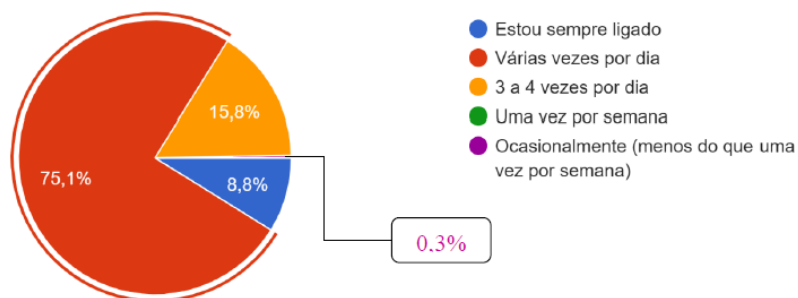


Gráfico 9 – A frequência online na aplicação favorita por dia

9. Ao aderir a uma rede ou quando compra equipamento tem o hábito de:

317 respostas

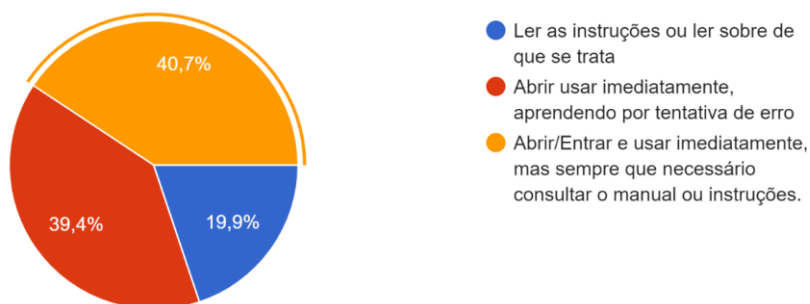


Gráfico 10 – Hábito de ler instruções ou aprender por tentativa de erro

10. Indique qual a informação que inclui no perfil da conta do seu Smartphone?

317 respostas

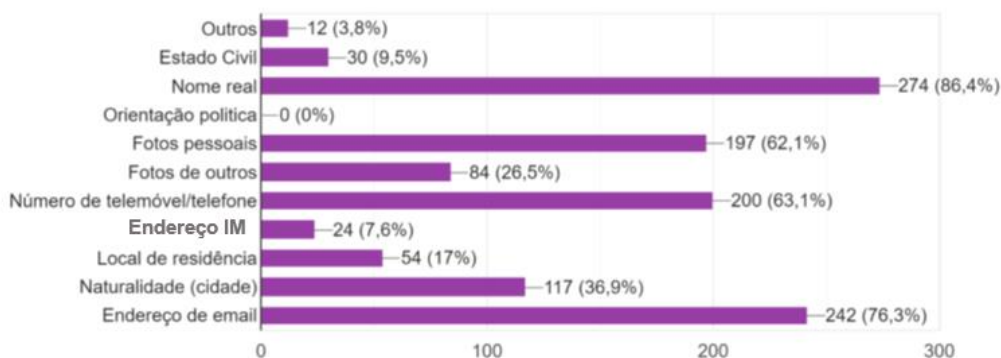


Gráfico 11 – Informações incluídas na conta do Smartphone pelos estudantes

11. Sabe que terceiros utilizam os seus dados pessoais que são registados pelo seu Smartphone?

317 respostas

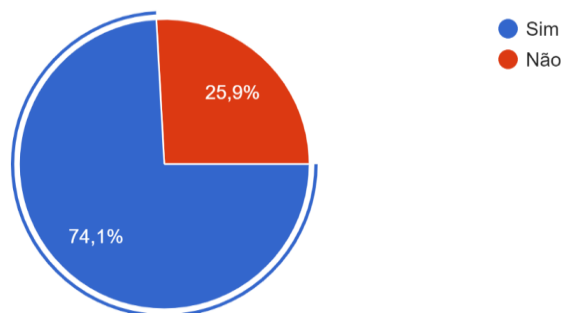


Gráfico 12 – Conhecimento dos estudantes sobre terceiros acederem aos seus dados registados pelo Smartphone

12. Aceita os termos de aceitação quando estes implicam ter acesso aos dados de posicionamento do seu Smartphone?

317 respostas

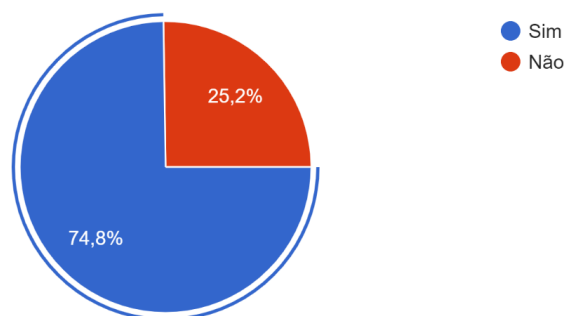


Gráfico 13 – Aceitação dos termos de aceitação com implicação dos dados de posicionamento do Smartphone

13. Na sua opinião, até que ponto sente que o Smartphone afecta os seus estudos?

317 respostas

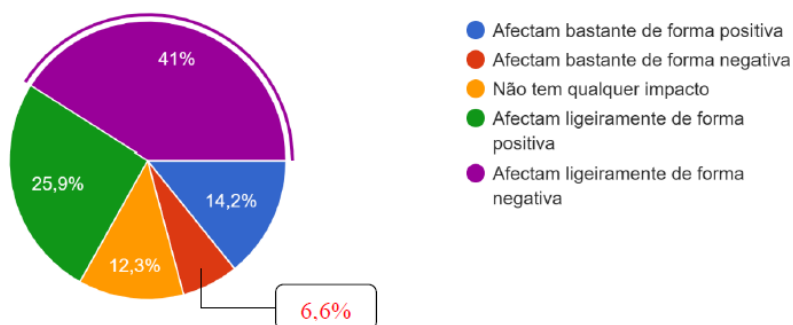


Gráfico 14 – Nível de afeto do Smartphone nos estudos dos estudantes

14. Numa escala de 1 a 5, previamente a ter um Smartphone, considerava que a utilização das apli...teriam riscos para a sua privacidade?

317 respostas

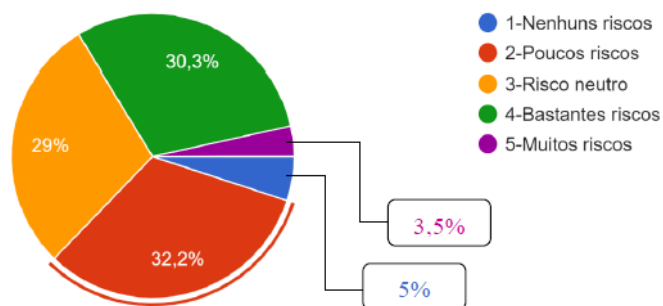


Gráfico 15 – Escala da percepção dos riscos de aplicações de comunicação antes da aquisição do Smartphone

15 - Numa escala de 1 a 5, previamente a ter um Smartphone, considerava que poderia confiar a pa... ao funcionamento deste dispositivo?

317 respostas

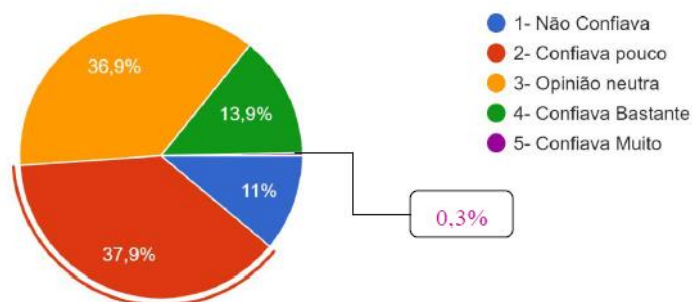


Gráfico 16 - Escala sobre a confiança da partilha de informação na utilização das aplicações antes da aquisição do Smartphone

16. Numa escala de 1 a 5, previamente a ter um Smartphone, considerava que a utilização do mesmo...os dados móveis que iria partilhar?

317 respostas

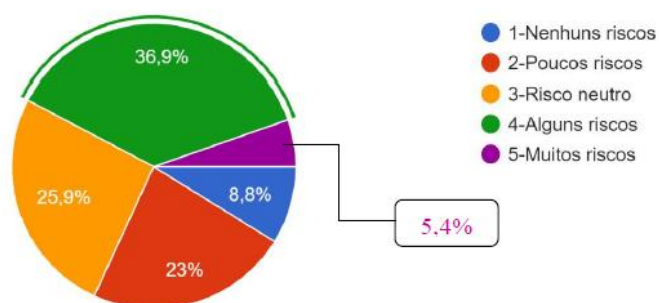


Gráfico 17 - Escala sobre a consideração dos riscos de privacidade na utilização do Smartphone antes da sua aquisição

17. Numa escala de 1 a 5, previamente a ter um Smartphone, considerava que a utilização da câmar...phone iria ter riscos de segurança?

317 respostas

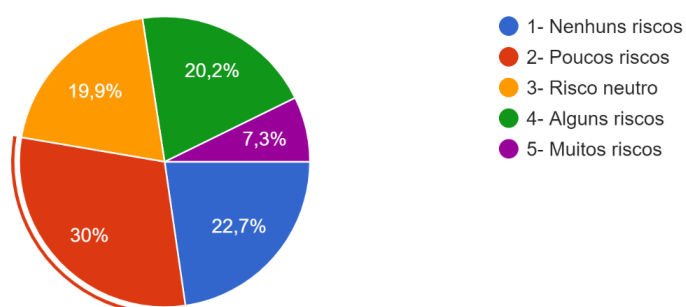


Gráfico 18 - Escala sobre a consideração dos riscos de privacidade na utilização da câmara do Smartphone

18. Numa escala de 1 a 5, previamente a ter um Smartphone, considerava que seria necessário inst...ando a utilização deste dispositivo?

317 respostas

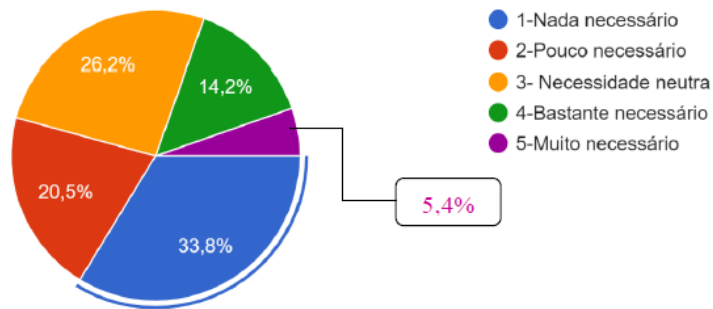


Gráfico 19 - Escala sobre a consideração se seria necessário instalar uma aplicação para proteger a sua privacidade

19. Houve alturas em que me preocupei com a minha privacidade ao utilizar o Smartphone?

317 respostas

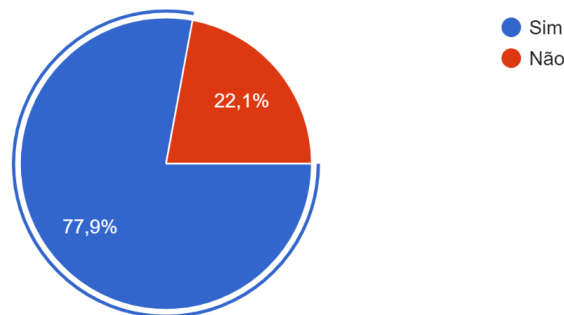


Gráfico 20 – Preocupação com a privacidade na utilização do Smartphone

20. Concorda em não comprar um Smartphone se pudesse voltar atrás?

317 respostas

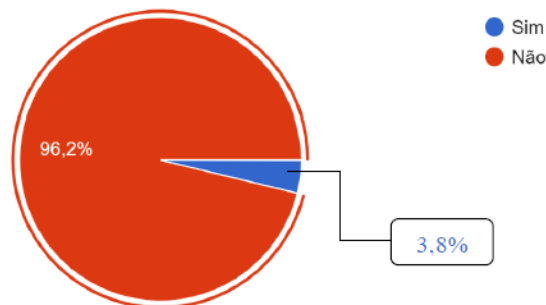


Gráfico 21 – Estudantes voltariam a comprar um Smartphone se pudessem voltar atrás

21. Algumas funcionalidades do Smartphone não são consistentes com as minhas expetativas antes da utilização?

317 respostas

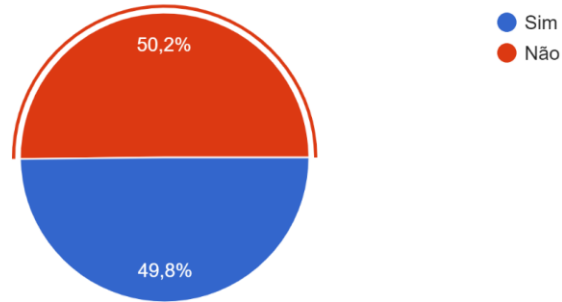


Gráfico 22 – Expetativas das funcionalidades do Smartphone com a realidade depois da utilização

22. Sempre tive a certeza de como era a utilização do Smartphone?

317 respostas

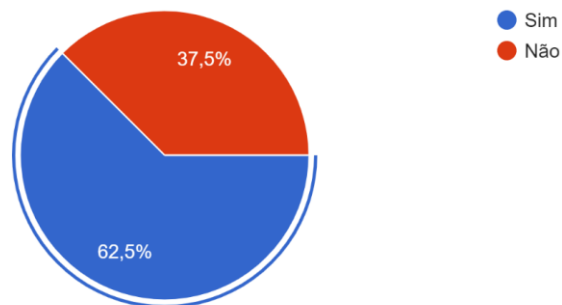


Gráfico 23 – Certeza sobre a utilização do Smartphone

23. Confiei no meu Smartphone?

317 respostas

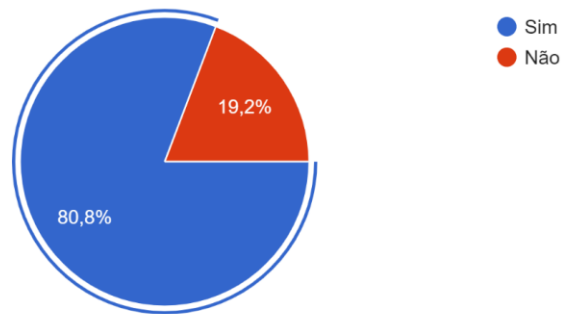


Gráfico 24 – Confiança no smartphone pessoal

24. Senti-me confortável ao usar o Smartphone?

317 respostas

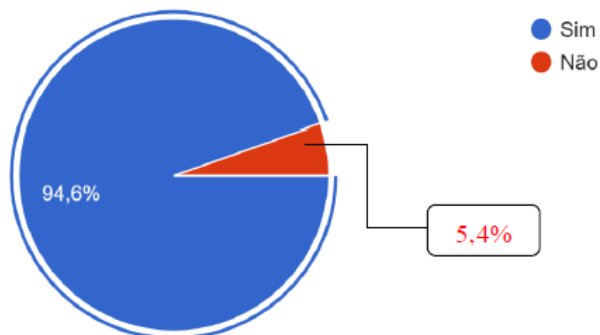


Gráfico 25 – Confortável ao usar o Smartphone

25. Utilizei bem o Smartphone?

317 respostas

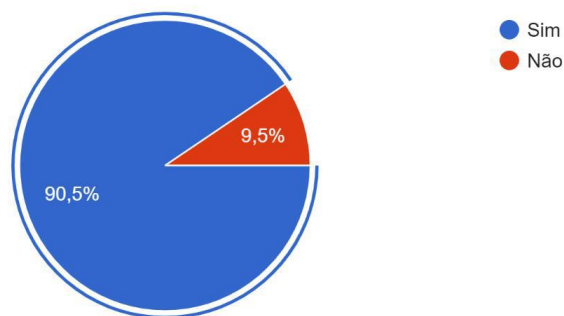


Gráfico 26 – Utilizei bem o Smartphone

26. Ao ter conhecimento dos riscos de segurança, vou parar de usar o Smartphone?

317 respostas

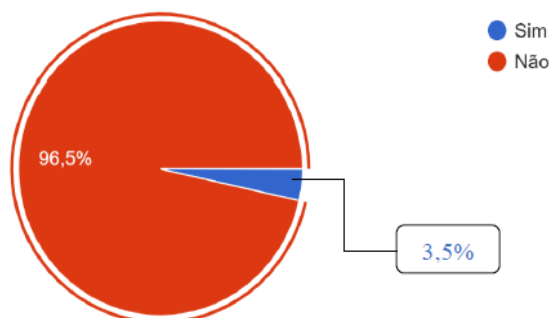


Gráfico 27 – Parar de utilizar smartphone conhecendo os riscos de segurança

27. Utiliza o Smartphone para uso académico?

317 respostas

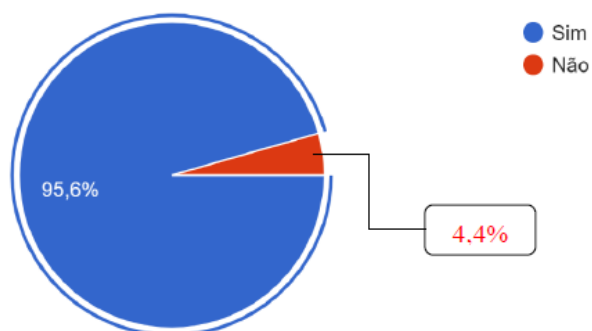


Gráfico 28 – Utilização do Smartphone para uso académico

28. Com que regularidade, em média, utiliza o Smartphone?

317 respostas

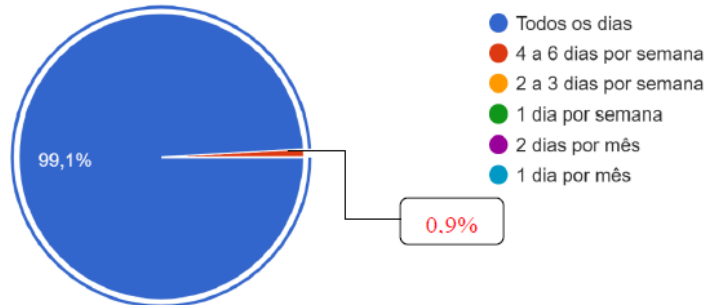


Gráfico 29 - Regularidade media de utilização

29. Em média, quanto tempo gasta, por dia, no Smartphone?

317 respostas

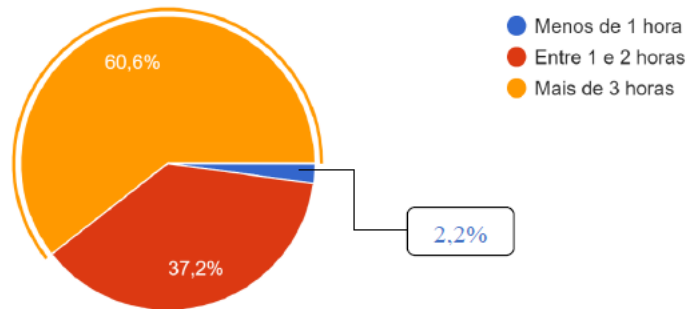


Gráfico 30 – Média de tempo por dia de utilização do Smartphone

30. Há quanto tempo possui um Smartphone?

317 respostas

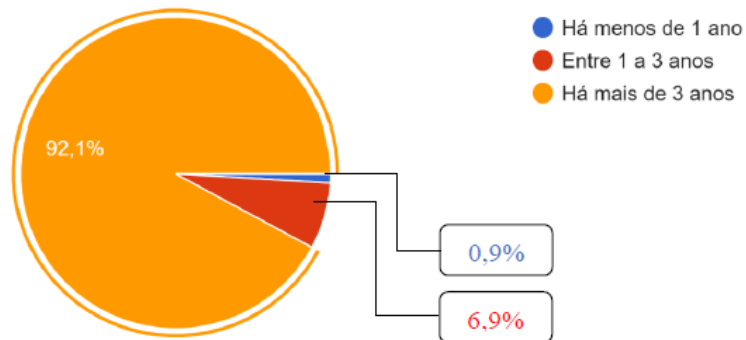


Gráfico 31 – Quantidade de anos em que possui um Smartphone

31. Em média, quantas horas por semana utiliza o Smartphone?

317 respostas

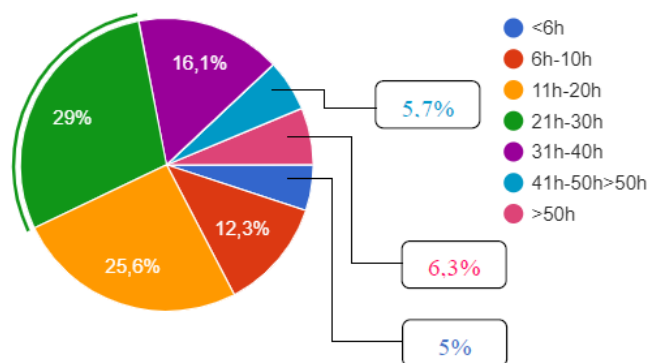


Gráfico 32 – Média de horas de utilização semanal com Smartphone

32. Numa escala de 1 a 5, considera que é fácil aprender a utilizar o Smartphone?

317 respostas

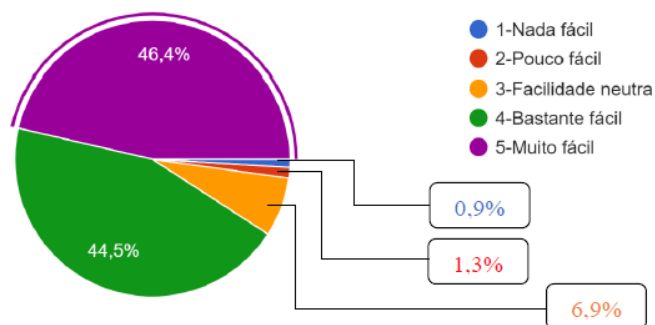


Gráfico 33 – Escala de dificuldade percebida ao aprender a utilizar o Smartphone

33. Numa escala de 1 a 5, considera que a utilização do Smartphone não requer muito esforço mental?

317 respostas

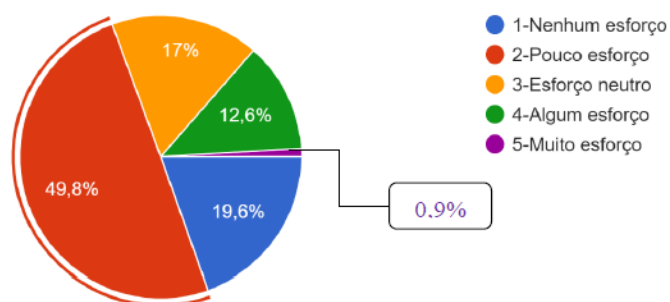


Gráfico 34 – Escala de nível de esforço mental requerido na utilização do Smartphone

34. Numa escala de 1 a 5, considera fácil comunicar com os seus contatos através do Smartphone?

317 respostas

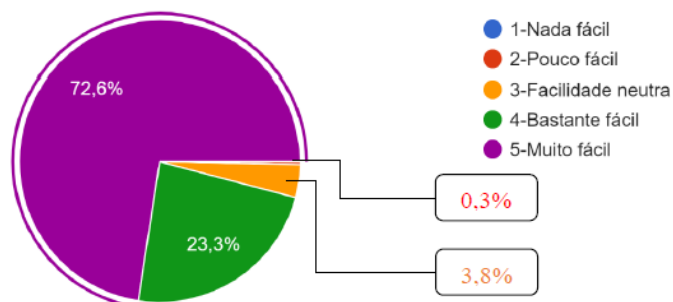


Gráfico 35 – Facilidade percebida para comunicar com os seus contactos através do Smartphone

35. As ferramentas do Smartphone são flexíveis para que eu possa usá-las da maneira que melhor me convier?

317 respostas

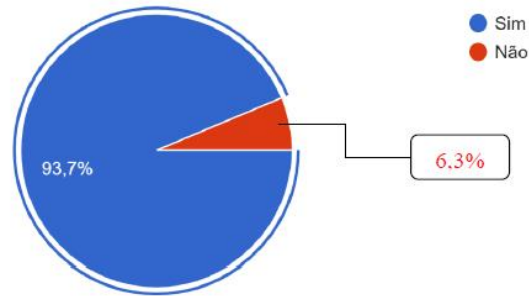


Gráfico 36 – Flexibilidade de ferramentas do Smartphone para poder utilizar

36. Numa escala de 1 a 5, considera fácil partilhar fotos/vídeos / estados no Smartphone?

317 respostas

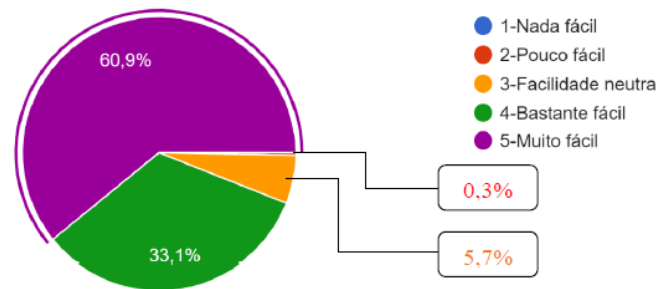


Gráfico 37 - Escala da consideração da facilidade percebida na partilha de fotos, vídeos e estados no Smartphone

37. Numa escala de 1 a 5, considera a interação com o Smartphone como flexível? (relativamente ao leque de aplicações disponíveis)

317 respostas

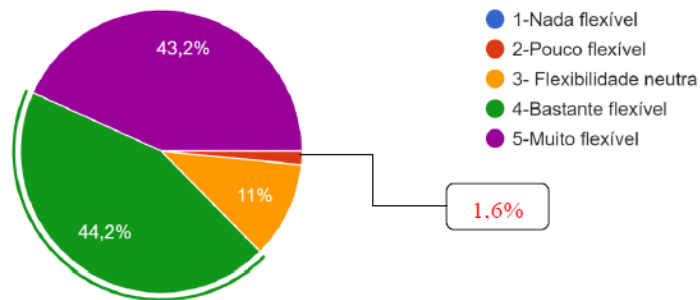


Gráfico 38 – Escala da consideração percebida da flexibilidade na interação com o Smartphone

38. Numa escala de 1 a 5, considera o Smartphone útil para comunicar com a sua rede de contactos pessoais (amigos)?

317 respostas

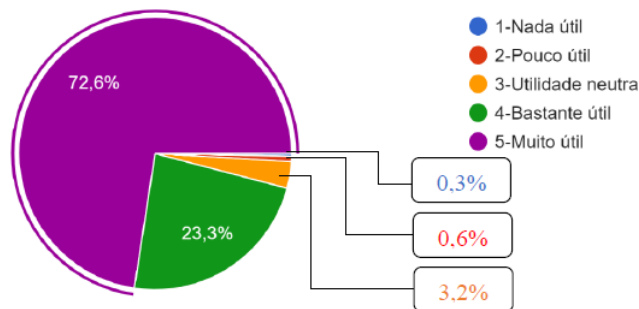


Gráfico 39 – Escala de consideração da utilidade percebida na comunicação da rede de contactos pessoais

39. Numa escala de 1 a 5, considera o Smartphone útil para comunicar com a sua rede de contactos universitários?

317 respostas

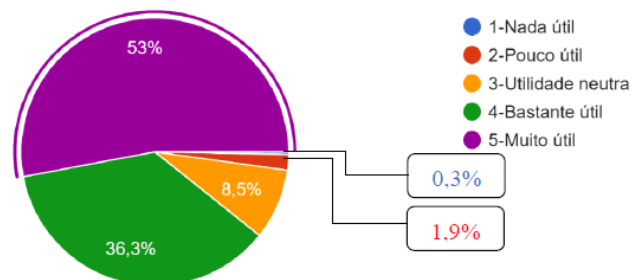


Gráfico 40 - Escala de consideração da utilidade percebida na comunicação da rede de contactos universitários

40. Numa escala de 1 a 5, considera útil ter a possibilidade de partilhar fotos/vídeos /ficheiros pelo Smartphone?

317 respostas

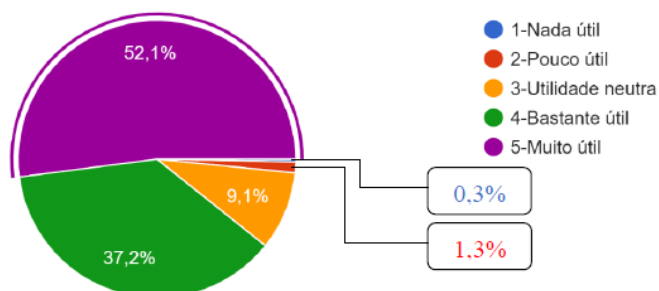


Gráfico 41 - Escala de consideração da utilidade percebida na partilha de fotos, videos e ficheiros através do Smartphone

41. Ao usar ferramentas do Smartphone o meu trabalho fica mais rápido?

317 respostas

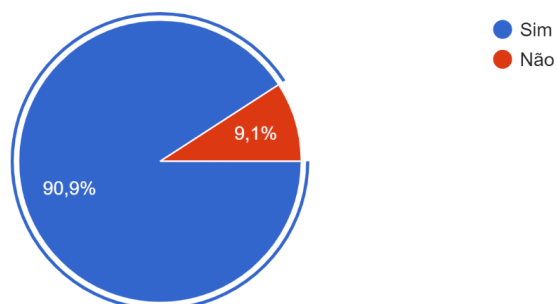


Gráfico 42 – Ferramentas de Smartphone como aumento de rapidez em trabalho

42. Usar o Smartphone aumenta a eficiência no trabalho do meu dia a dia?

317 respostas

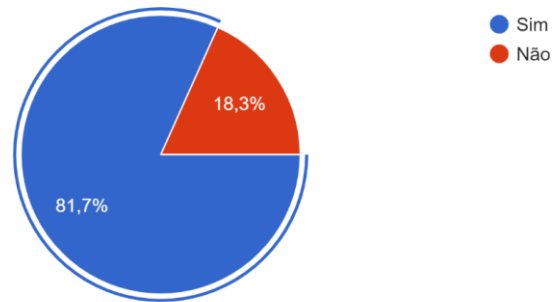


Gráfico 43 – Aumento da eficiência no trabalho diário com uso do Smartphone

43. Numa escala de 1 a 5, indique até que ponto sente que o Smartphone o afeta os seus estudos:

317 respostas

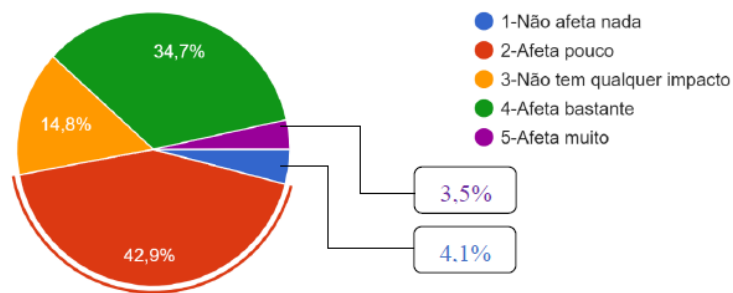


Gráfico 44 – Escala de afeto sentido pelo Smartphone nos estudos

44. Numa escala de 1 a 5, previamente a ter um Smartphone, considerava que a utilização do Smartphone iria ser útil nos seus estudos?

317 respostas

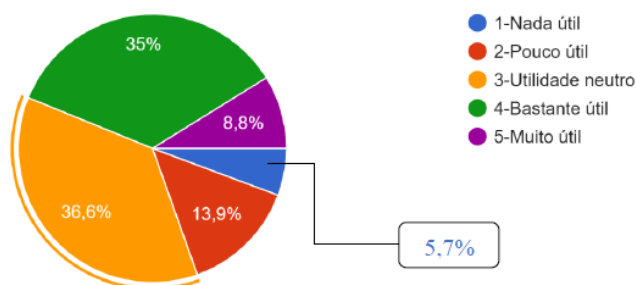


Gráfico 45 – Escala sobre a consideração se Smartphone iria ser útil para os estudos, previamente a possuir um

45. Quero utilizar o Smartphone, sempre que possível.

317 respostas

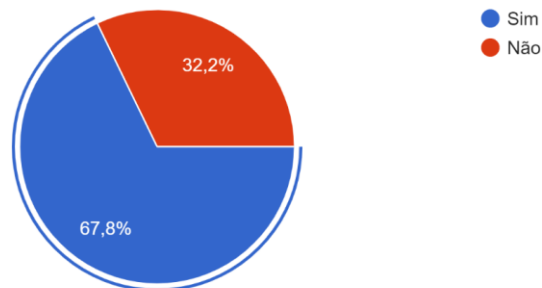


Gráfico 46 – Utilizar o Smartphone sempre que possível

46. Tenho a intenção de aumentar o uso das ferramentas no Smartphone?

317 respostas

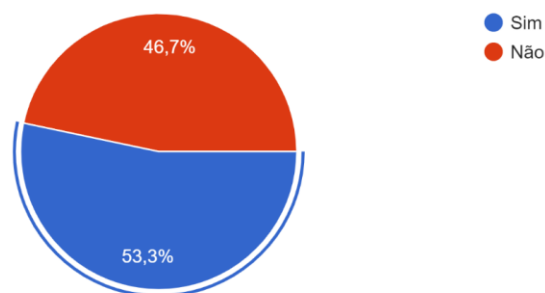


Gráfico 47 – Intenções de aumentar o uso das ferramentas dos Smartphone

47. Adorava ter novas ferramentas no meu Smartphone, no futuro?

317 respostas

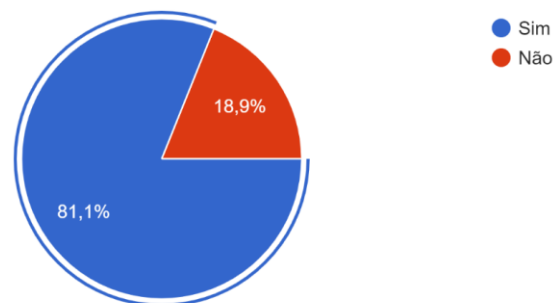


Gráfico 48 – Desejo de ter novas ferramentas no Smartphone

48. Tenho necessidade de tapar a câmara do Smartphone em algumas situações.

317 respostas

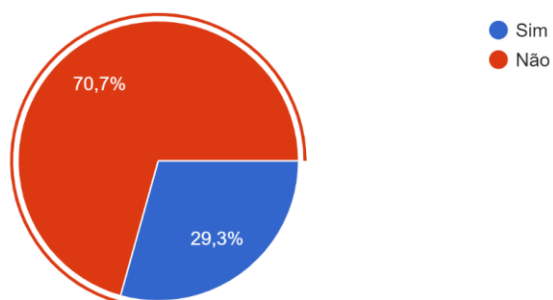


Gráfico 49 – Necessidade de tapar a câmara do Smartphone

49. Tenho necessidade de desligar o GPS sempre que não precisa?

317 respostas

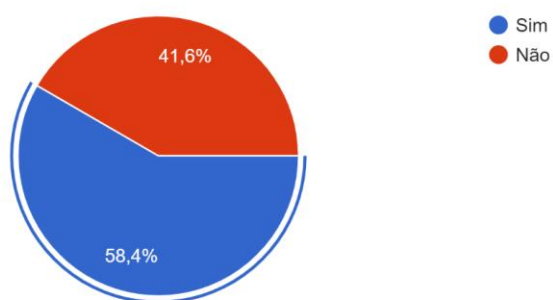


Gráfico 50 – Necessidade de desligar o GPS sempre não utiliza

50. Sinto necessidade de desligar o Smartphone por completo durante os períodos em que não o estou a usar, por questões de segurança?

317 respostas

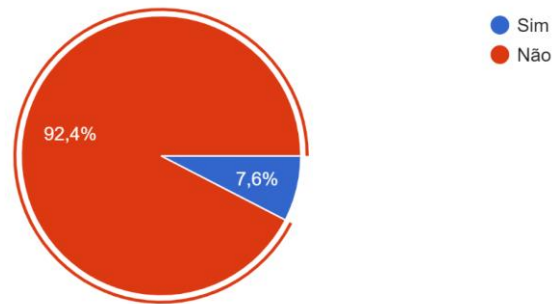


Gráfico 51 – Necessidade de desligar o Smartphone quando não se está a utilizar por questões de segurança

51. Tenho intenção de adquirir uma aplicação para me defender da invasão de terceiros?

317 respostas

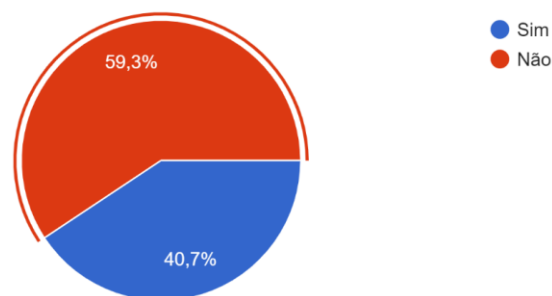


Gráfico 52 – Intenções de aquisição de aplicativo para proteção de invasão por terceiros

52. Adorava ter um botão que me permitisse ligar e desligar o microfone do meu Smartphone.

317 respostas

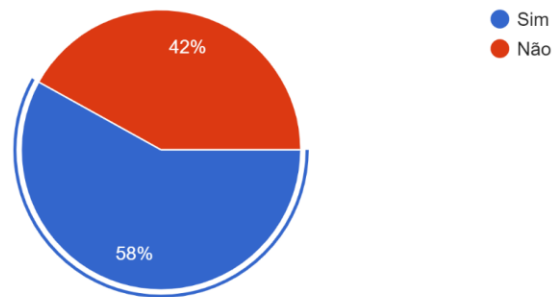


Gráfico 53 – Desejo de botão que permite desligar o microfone do Smartphone

53. Indique quais destas aplicações usa frequentemente no seu Smartphone?

317 respostas

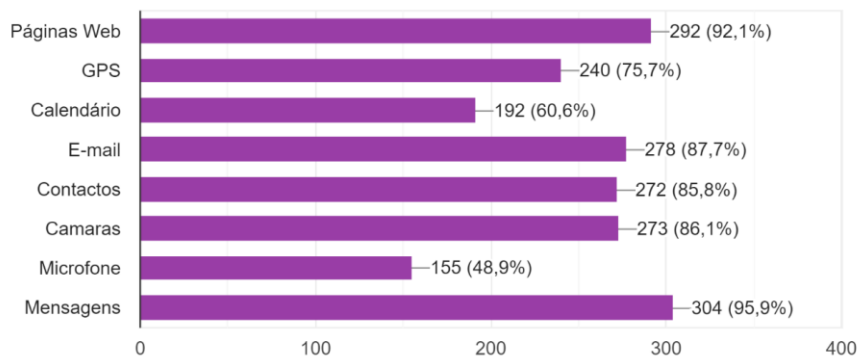


Gráfico 54 – Aplicações de uso frequente no Smartphone

54. Com que frequência usa ferramentas do Smartphone?

317 respostas

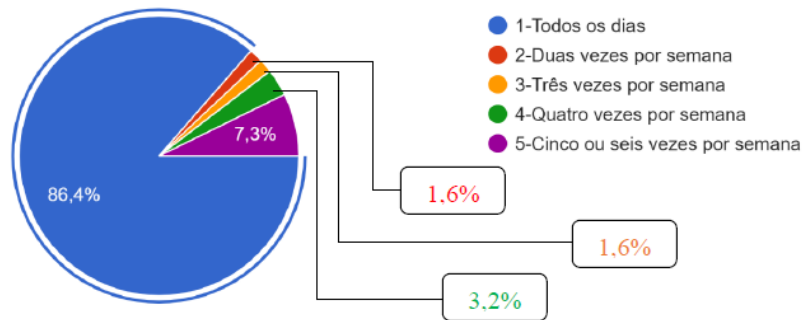


Gráfico 55 – Frequência do uso de ferramentas do Smartphone

55. Costumo usar o meu smartphone para partilhar dados/fotografias.

317 respostas

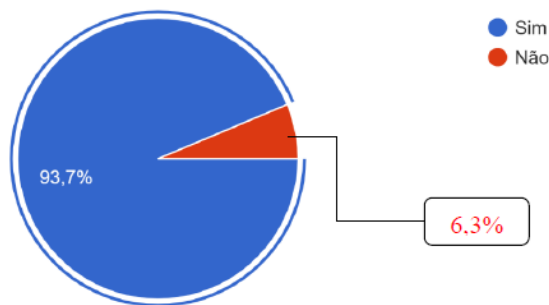


Gráfico 56 – Habitualmente usa o Smartphone para partilhar dados/fotografias

56. Costuma usar o smartphone para monitorizar a sua atividade física/desportiva?

317 respostas

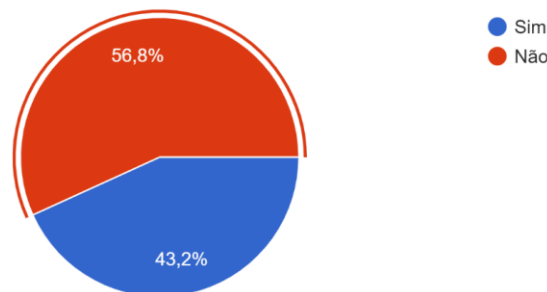


Gráfico 57 – Uso do Smartphone para monitorizar a atividade física/desportiva

57. Costuma usar o GPS do seu smartphone para atividades físicas?

317 respostas

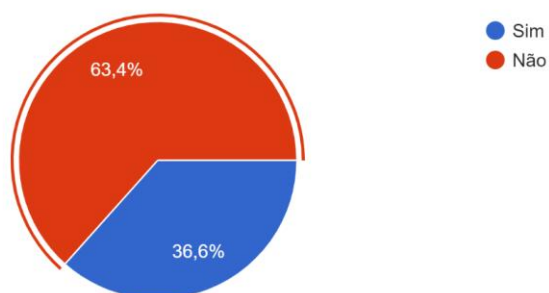


Gráfico 58 – Uso do GPS para atividades físicas

58. Divulga as suas informações pessoais no Smartphone?

317 respostas

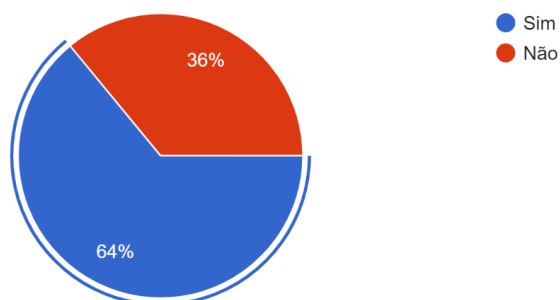


Gráfico 59 – Divulgação de informações pessoais pelo Smartphone

59. Numa escala de 1 a 5, considera o Smartphone um meio seguro para partilhar fotos/ vídeos/ ficheiros/ informações pessoais?

317 respostas

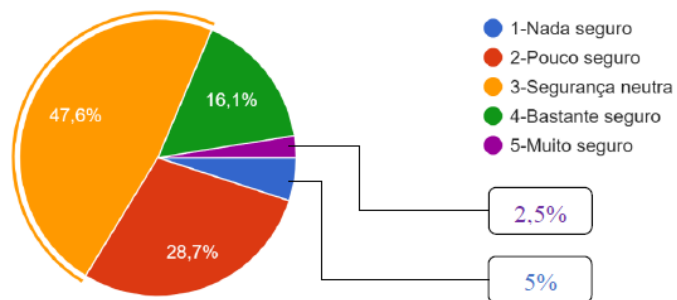


Gráfico 60 – Segurança na partilha de fotos/ficheiros/informações pessoais com Smartphone

60. No geral, e numa escala de 1 a 5, sente-se plenamente seguro em utilizar o Smartphone, para comunicar com os seus contactos ou empresas?

317 respostas

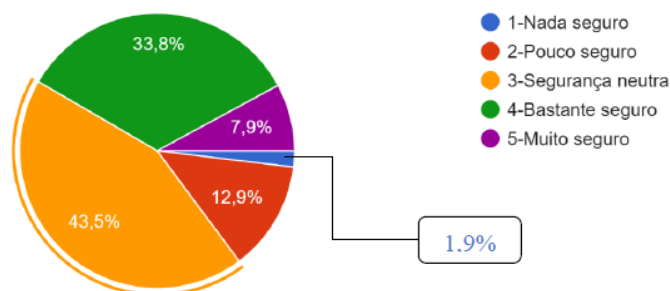


Gráfico 61 – Escala sobre segurança com smartphone na comunicação com contactos ou empresas

61. No geral, e numa escala de 1 a 5, sente-se plenamente seguro em utilizar o Smartphone para jogar as m...ções disponibilizadas no Smartphone?

317 respostas

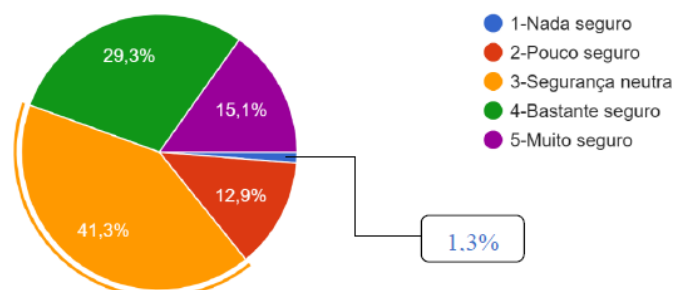


Gráfico 62 – Escala sobre segurança com smartphone para jogar as mais diversas aplicações

62. Sente-se seguro a utilizar o Smartphone para ter conversas privadas, relacionadas com o trabalho ou dados sensíveis?

317 respostas

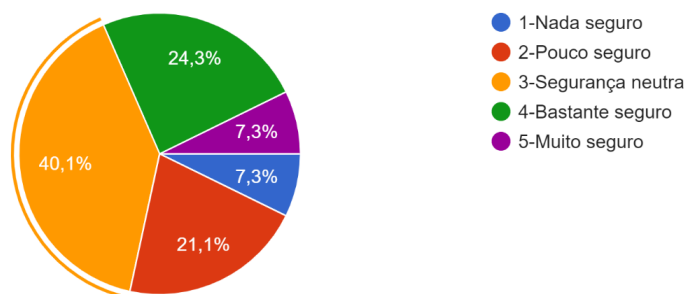


Gráfico 63 – Segurança ao utilizar Smartphone em conversas privadas ou dados sensíveis

Apêndice B – Tabelas SPSS por pergunta de investigação

Tabelas da análise quantitativa com SPSS

Grupo 3				
Item	Cruzamento	χ^2	<i>sig</i>	<i>V</i>
14	Utilização de aplicações tem risco	5.74	0.219	0.135
15	Confia a partilha de informação	9.07	0.059	0.169**
16	Utilização do mesmo tem risco aos dados móveis	8.47	0.076	0.163**
17	Utilização da câmara tem risco de segurança	5.11	0.276	0.127
18	Instalar uma aplicação para manter a privacidade	8.77	0.067	0.166**
Grupo 4				
Item	Cruzamento	χ^2	<i>sig</i>	<i>V</i>
19	Houve alturas que se preocupou com a privacidade	4.76	0.030	0.122*
20	Não comprava um <i>Smartphone</i> se voltasse atrás	3.25	0.112	0.101**
21	As funcionalidades não são consistentes como esperava	1.00	0.338	0.056
23	Confia no <i>Smartphone</i>	6.52	0.014	0.143*
24	Sente-se confortável ao usar o <i>Smartphone</i>	3.55	0.067	0.106**
25	Utiliza bem o <i>Smartphone</i>	0.31	0.682	0.031
Grupo 8				
Item	Cruzamento	χ^2	<i>sig</i>	<i>V</i>
48	Necessidade de tapar a câmara do <i>Smartphone</i>	28.10	0.001	0.298*
49	Necessidade de desligar o GPS	0.36	0.626	0.034
50	Desligar o <i>Smartphone</i> no momento que não utiliza	4.61	0.039	0.121*
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.52	0.142	0.089
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	1.99	0.181	0.079
Grupo 10				
Item	Cruzamento	χ^2	<i>sig</i>	<i>V</i>
58	Divulga informações pessoais no <i>Smartphone</i>	1.78	0.211	0.075
59	Considera seguro de partilhar multimédia	6.56	0.161	0.144
60	Sente seguro para comunicar-se com contactos e empresa	6.46	0.167	0.143
61	Sente seguro para jogar em diversas aplicações	6.95	0.139	0.148

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 4 – Teste Qui-quadrado e V de Crámer por sexo dos estudantes

Sexo			I.C	
Item	Cruzamento	O.R	Inferior	Superior
19	Houve alturas que se preocupou com a privacidade	0.50*	0.27	0.94
20	Não comprava um <i>Smartphone</i> se voltasse atrás	5.45	0.69	42.77
23	Confia no <i>Smartphone</i>	2.08*	1.18	3.70
48	Necessidade de tapar a câmara do <i>Smartphone</i>	0.26*	0.16	0.43
50	Desligar o <i>Smartphone</i> no momento que não utiliza	3.57*	1.04	12.27

Nota: * Significativo ao nível de 5% ($\alpha = 0.05$); O.R: *Odds Ratio*; I.C: Intervalo de Confiança

Tabela 5 – Razão de chance (Odds Ratio) por Sexo dos estudantes

Grupo 3				
Item	Cruzamento	χ^2	sig	V
14	Utilização de aplicações tem risco	3.97	0.410	0.112
15	Confia a partilha de informação	10.77	0.029	0.184*
16	Utilização do mesmo tem risco aos dados móveis	4.24	0.375	0.116
17	Utilização da câmara tem risco de segurança	12.99	0.011	0.202*
18	Instalar uma aplicação para manter a privacidade	11.38	0.023	0.189*

Grupo 4				
Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	0.74	0.399	0.048
20	Não comprava um <i>Smartphone</i> se voltasse atrás	0.20	0.761	0.025
21	As funcionalidades não são consistentes como esperava	1.20	0.293	0.062
23	Confia no <i>Smartphone</i>	0.27	0.657	0.029
24	Sente-se confortável ao usar o <i>Smartphone</i>	0.30	0.795	0.031
25	Utiliza bem o <i>Smartphone</i>	0.02	1.000	0.007

Grupo 8				
Item	Cruzamento	χ^2	sig	V
48	Necessidade de tapar a câmara do <i>Smartphone</i>	0.00	1.000	0.002
49	Necessidade de desligar o GPS	0.05	0.905	0.013
50	Desligar o <i>Smartphone</i> no momento que não utiliza	1.12	0.278	0.061

51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	0.23	0.635	0.027
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	0.11	0.812	0.019

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	0.79	0.395	0.050
59	Considera seguro de partilhar multimédia	0.63	0.960	0.044
60	Sente seguro para comunicar-se com contactos e empresa	7.14	0.128	0.150
61	Sente seguro para jogar em diversas aplicações	2.19	0.701	0.083

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 6 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 3

Item	Cruzamento	χ^2	sig	V
14	Utilização de aplicações tem risco	-	-	0.082
15	Confia a partilha de informação	-	-	0.080
16	Utilização do mesmo tem risco aos dados móveis	-	-	0.119
17	Utilização da câmara tem risco de segurança	-	-	0.120
18	Instalar uma aplicação para manter a privacidade	-	-	0.121

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	1.26	0.869	0.063
20	Não comprava um <i>Smartphone</i> se voltasse atrás	-	-	0.125
21	As funcionalidades não são consistentes como esperava	2.28	0.685	0.085
23	Confia no <i>Smartphone</i>	3.98	0.409	0.112
24	Sente-se confortável ao usar o <i>Smartphone</i>	-	-	0.186*
25	Utiliza bem o <i>Smartphone</i>	-	-	0.078

Grupo 8

Item	Cruzamento	χ^2	sig	V
48	Necessidade de tapar a câmara do <i>Smartphone</i>	4.37	0.358	0.117
49	Necessidade de desligar o GPS	3.12	0.538	0.099

50	Desligar o <i>Smartphone</i> no momento que não utiliza	-	-	0.088
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.32	0.678	0.085
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	5.40	0.248	0.131

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	4.24	0.374	0.116
59	Considera seguro de partilhar multimédia	-	-	0.169*
60	Sente seguro para comunicar-se com contactos e empresa	-	-	0.138**
61	Sente seguro para jogar em diversas aplicações	-	-	0.132

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 7 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Grupo 3

Item	Cruzamento	χ^2	sig	V
14	Utilização de aplicações tem risco	5.74	0.219	0.135
15	Confia a partilha de informação	9.07	0.059	0.169**
16	Utilização do mesmo tem risco aos dados móveis	8.47	0.076	0.163**
17	Utilização da câmara tem risco de segurança	5.11	0.276	0.127
18	Instalar uma aplicação para manter a privacidade	8.77	0.067	0.166**

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	5.74	0.219	0.135
23	Confia no <i>Smartphone</i>	6.52	0.014	0.143*
24	Sente-se confortável ao usar o <i>Smartphone</i>	3.55	0.067	0.106**
25	Utiliza bem o <i>Smartphone</i>	0.31	0.682	0.031

Grupo 8

Item	Cruzamento	χ^2	sig	V
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	15.58	0.001	0.222*
47	Adorava ter novas ferramentas no <i>Smartphone</i>	10.77	0.002	0.184*

48	Necessidade de tapar a câmara do <i>Smartphone</i>	28.10	0.001	0.298*
49	Necessidade de desligar o GPS	0.36	0.626	0.034
50	Desligar o <i>Smartphone</i> no momento que não utiliza	4.61	0.039	0.121*
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.52	0.142	0.089
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	1.99	0.181	0.079

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	1.78	0.211	0.075
59	Considera seguro de partilhar multimédia	6.56	0.161	0.144
60	Sente seguro para comunicar-se com contactos e empresa	6.46	0.167	0.143
61	Sente seguro para jogar em diversas aplicações	6.95	0.139	0.148

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 8 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes

Sexo			I.C	
Item	Cruzamento	O.R	Inferior	Superior
23	Confia no <i>Smartphone</i>	2.08*	1.18	3.70
24	Sente-se confortável ao usar o <i>Smartphone</i>	2.50	0.94	6.70
46	Intenção de aumentar uso das ferramentas do <i>Smartphone</i>	2.63*	1.62	4.27
47	Adorava ter novas ferramentas no <i>Smartphone</i>	2.57*	1.45	4.57
48	Necessidade de tapar a câmara do <i>Smartphone</i>	0.26	0.16	0.43
50	Desligar o <i>Smartphone</i> no momento que não utiliza	3.57	1.04	12.27

Nota: * Significativo ao nível de 5% ($\alpha = 0,05$); O.R: *Odds Ratio*; I.C: Intervalo de Confiança

Tabela 9 - Razão de chance (*Odds Ratio*) por Sexo dos estudantes

Grupo 3

Item	Cruzamento	χ^2	sig	V
14	Utilização de aplicações tem risco	3.97	0.410	0.112
15	Confia a partilha de informação	10.77	0.029	0.184*
16	Utilização do mesmo tem risco aos dados móveis	4.24	0.375	0.116

17	Utilização da câmara tem risco de segurança	12.99	0.011	0.202*
18	Instalar uma aplicação para manter a privacidade	11.38	0.023	0.189*

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	0.74	0.399	0.048
23	Confia no <i>Smartphone</i>	0.27	0.657	0.029
24	Sente-se confortável ao usar o <i>Smartphone</i>	0.30	0.795	0.031
25	Utiliza bem o <i>Smartphone</i>	0.02	1.000	0.007

Grupo 8

Item	Cruzamento	χ^2	sig	V
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	4.24	0.046	0.116*
47	Adorava ter novas ferramentas no <i>Smartphone</i>	0.17	0.765	0.023
48	Necessidade de tapar a câmara do <i>Smartphone</i>	0.00	1.000	0.002
49	Necessidade de desligar o GPS	0.05	0.905	0.013
50	Desligar o <i>Smartphone</i> no momento que não utiliza	1.12	0.278	0.061
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	0.23	0.635	0.027
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	0.11	0.812	0.019

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	0.79	0.395	0.050
59	Considera seguro de partilhar multimédia	0.63	0.960	0.044
60	Sente seguro para comunicar-se com contactos e empresa	7.14	0.128	0.150
61	Sente seguro para jogar em diversas aplicações	2.19	0.701	0.083

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 10 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 3

Item	Cruzamento	χ^2	sig	V
14	Utilização de aplicações tem risco	-	-	0.082
15	Confia a partilha de informação	-	-	0.080

16	Utilização do mesmo tem risco aos dados móveis	-	-	0.119
17	Utilização da câmara tem risco de segurança	-	-	0.120
18	Instalar uma aplicação para manter a privacidade	-	-	0.121

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	1.26	0.869	0.063
23	Confia no <i>Smartphone</i>	3.98	0.409	0.112
24	Sente-se confortável ao usar o <i>Smartphone</i>	-	-	0.186*
25	Utiliza bem o <i>Smartphone</i>	-	-	0.078

Grupo 8

Item	Cruzamento	χ^2	sig	V
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	7.53	0.110	0.154
47	Adorava ter novas ferramentas no <i>Smartphone</i>	1.60	0.810	0.071
48	Necessidade de tapar a câmara do <i>Smartphone</i>	4.37	0.358	0.117
49	Necessidade de desligar o GPS	3.12	0.538	0.099
50	Desligar o <i>Smartphone</i> no momento que não utiliza	-	-	0.088
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.32	0.678	0.085
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	5.40	0.248	0.131

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	4.24	0.374	0.116
59	Considera seguro de partilhar multimédia	-	-	0.169*
60	Sente seguro para comunicar-se com contactos e empresa	-	-	0.138**
61	Sente seguro para jogar em diversas aplicações	-	-	0.132

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 11 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Grupo 3

Item	Cruzamento	χ^2	sig	V
15	Confia a partilha de informação	9.07	0.059	0.169**

16	Utilização do mesmo tem risco aos dados móveis	8.47	0.076	0.163**
17	Utilização da câmara tem risco de segurança	5.11	0.276	0.127
18	Instalar uma aplicação para manter a privacidade	8.77	0.067	0.166**

Grupo 8

Item	Cruzamento	χ^2	sig	V
48	Necessidade de tapar a câmara do <i>Smartphone</i>	28.10	0.001	0.298*
49	Necessidade de desligar o GPS	0.36	0.626	0.034
50	Desligar o <i>Smartphone</i> no momento que não utiliza	4.61	0.039	0.121*
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.52	0.142	0.089
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	1.99	0.181	0.079

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	1.78	0.211	0.075
59	Considera seguro de partilhar multimédia	6.56	0.161	0.144
60	Sente seguro para comunicar-se com contactos e empresa	6.46	0.167	0.143
61	Sente seguro para jogar em diversas aplicações	6.95	0.139	0.148

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 12 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes

Sexo		I.C		
Item	Cruzamento	O.R	Inferior	Superior
48	Necessidade de tapar a câmara do <i>Smartphone</i>	0.26*	0.16	0.43
50	Desligar o <i>Smartphone</i> no momento que não utiliza	3.57*	1.04	12.27

Nota: * Significativo ao nível de 5% ($\alpha = 0,05$); O.R: *Odds Ratio*; I.C: Intervalo de Confiança

Tabela 13 - Razão de chance (Odds Ratio) por Sexo dos estudantes

Grupo 3

Item	Cruzamento	χ^2	sig	V
15	Confia a partilha de informação	10.77	0.029	0.184*
16	Utilização do mesmo tem risco aos dados móveis	4.24	0.375	0.116
17	Utilização da câmara tem risco de segurança	12.99	0.011	0.202*
18	Instalar uma aplicação para manter a privacidade	11.38	0.023	0.189*

Grupo 8

Item	Cruzamento	χ^2	sig	V
48	Necessidade de tapar a câmara do <i>Smartphone</i>	0.00	1.000	0.002
49	Necessidade de desligar o GPS	0.05	0.905	0.013
50	Desligar o <i>Smartphone</i> no momento que não utiliza	1.12	0.278	0.061
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	0.23	0.635	0.027
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	0.11	0.812	0.019

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	0.79	0.395	0.050
59	Considera seguro de partilhar multimédia	0.63	0.960	0.044
60	Sente seguro para comunicar-se com contactos e empresa	7.14	0.128	0.150
61	Sente seguro para jogar em diversas aplicações	2.19	0.701	0.083

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 14 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 3

Item	Cruzamento	χ^2	sig	V
15	Confia a partilha de informação	-	-	0.080
16	Utilização do mesmo tem risco aos dados móveis	-	-	0.119
17	Utilização da câmara tem risco de segurança	-	-	0.120
18	Instalar uma aplicação para manter a privacidade	-	-	0.121

Grupo 8

Item	Cruzamento	χ^2	sig	V
48	Necessidade de tapar a câmara do <i>Smartphone</i>	4.37	0.358	0.117
49	Necessidade de desligar o GPS	3.12	0.538	0.099
50	Desligar o <i>Smartphone</i> no momento que não utiliza	-	-	0.088
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.32	0.678	0.085
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	5.40	0.248	0.131

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	4.24	0.374	0.116
59	Considera seguro de partilhar multimédia	-	-	0.169*
60	Sente seguro para comunicar-se com contactos e empresa	-	-	0.138**
61	Sente seguro para jogar em diversas aplicações	-	-	0.132

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 15 – Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Grupo 8

Item	Cruzamento	χ^2	sig	V
47	Adorava ter novas ferramentas no <i>Smartphone</i>	10.77	0.002	0.184*
48	Necessidade de tapar a câmara do <i>Smartphone</i>	28.10	0.001	0.298*
49	Necessidade de desligar o GPS	0.36	0.626	0.034
50	Desligar o <i>Smartphone</i> no momento que não utiliza	4.61	0.039	0.121*
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.52	0.142	0.089
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	1.99	0.181	0.079

Grupo 9

Item	Cruzamento	χ^2	sig	V
57	Usa GPS para atividades físicas e desportivas	5,42	0,024	0.131*

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 16 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes

Sexo			I.C	
Item	Cruzamento	O.R	Inferior	Superior
47	Adorava ter novas ferramentas no <i>Smartphone</i>	2.57*	1.45	4.57
48	Necessidade de tapar a câmara do <i>Smartphone</i>	0.26*	0.16	0.43
50	Desligar o <i>Smartphone</i> no momento que não utiliza	3.57*	1.04	12.27
57	Usa GPS para atividades físicas e desportivas	1,83*	1,10	3,06

Nota: * Significativo ao nível de 5% ($\alpha = 0.05$); O.R: *Odds Ratio*; I.C: Intervalo de Confiança

Tabela 17 - Razão de chance (*Odds Ratio*) por Sexo dos estudantes

Grupo 8				
Item	Cruzamento	χ^2	sig	V
47	Adorava ter novas ferramentas no <i>Smartphone</i>	0.17	0.765	0.023
48	Necessidade de tapar a câmara do <i>Smartphone</i>	0.00	1.000	0.002
49	Necessidade de desligar o GPS	0.05	0.905	0.013
50	Desligar o <i>Smartphone</i> no momento que não utiliza	1.12	0.278	0.061
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	0.23	0.635	0.027
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	0.11	0.812	0.019

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 18 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 8				
Item	Cruzamento	χ^2	sig	V
47	Adorava ter novas ferramentas no <i>Smartphone</i>	1.60	0.810	0.071
48	Necessidade de tapar a câmara do <i>Smartphone</i>	4.37	0.358	0.117
49	Necessidade de desligar o GPS	3.12	0.538	0.099
50	Desligar o <i>Smartphone</i> no momento que não utiliza	-	-	0.088

51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.32	0.678	0.085
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	5.40	0.248	0.131

Grupo 9

Item	Cruzamento	χ^2	sig	V
57	Usa GPS para atividades físicas e desportivas	5,70	0,223	0,134

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 19 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Grupo 2

Item	Cruzamento	χ^2	sig	V
11	Terceiros utilizam os dados	2.38	0.132	0.087
12	Aceita termos de aceitação	8.06	0.006	0.159*

Grupo 3

Item	Cruzamento	χ^2	sig	V
15	Confia a partilha de informação	9.07	0.059	0.169**
16	Utilização do mesmo tem risco aos dados móveis	8.47	0.076	0.163**
17	Utilização da câmara tem risco de segurança	5.11	0.276	0.127
18	Instalar uma aplicação para manter a privacidade	8.77	0.067	0.166**

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	4.76	0.030	0.122*
26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	2.78	0.113	0.094**

Grupo 7

Item	Cruzamento	χ^2	sig	V
40	Considera útil ter possibilidade de partilhar multimédia	-	-	0.103

Grupo 9

Item	Cruzamento	χ^2	sig	V
55	Costuma usar <i>Smartphone</i> para partilhar multimédia	4.81	0.027	0.123*
56	Monitorizar atividade física/desportiva	0.98	0.334	0.056

57	Usa GPS para atividades físicas e desportivas	5.42	0.024	0.131*
----	---	------	-------	--------

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	1.78	0.211	0.075
59	Considera seguro de compartilhar multimídia	6.56	0.161	0.144
60	Sente seguro para comunicar-se com contactos e empresa	6.46	0.167	0.143
61	Sente seguro para jogar em diversas aplicações	6.95	0.139	0.148

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 20 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes

Item	Cruzamento	Sexo	I.C	
			O.R	Inferior
12	Aceita termos de aceitação	2.12*	1.26	3.58
19	Houve alturas que se preocupou com a privacidade	0.50*	0.27	0.94
55	Costuma usar <i>Smartphone</i> para partilhar multimídia	0.22*	0.05	0.96
57	Usa GPS para atividades físicas e desportivas	1.83*	1.10	3.06

Nota: * Significativo ao nível de 5% ($\alpha = 0.05$); O.R: *Odds Ratio*; I.C: Intervalo de Confiança

Tabela 21 - Razão de chance (Odds Ratio) por Sexo dos estudantes

Grupo 2

Item	Cruzamento	χ^2	sig	V
11	Terceiros utilizam os dados	3.75	0.061	0.109*
12	Aceita termos de aceitação	0.46	0.589	0.038

Grupo 3

Item	Cruzamento	χ^2	sig	V
15	Confia a partilha de informação	10.77	0.029	0.184*
16	Utilização do mesmo tem risco aos dados móveis	4.24	0.375	0.116
17	Utilização da câmara tem risco de segurança	12.99	0.011	0.202*
18	Instalar uma aplicação para manter a privacidade	11.38	0.023	0.189*

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	0.74	0.399	0.048
26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	3.89	0.059	0.111*

Grupo 7

Item	Cruzamento	χ^2	sig	V
40	Considera útil ter possibilidade de partilhar multimídia	-	-	0.169

Grupo 9

Item	Cruzamento	χ^2	sig	V
55	Costuma usar <i>Smartphone</i> para partilhar multimídia	0.81	0.470	0.051
56	Monitorizar atividade física/desportiva	1.49	0.238	0.069
57	Usa GPS para atividades físicas e desportivas	3.47	0.069	0.105**

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	0.79	0.395	0.050
59	Considera seguro de compartilhar multimídia	0.63	0.960	0.044
60	Sente seguro para comunicar-se com contactos e empresa	7.14	0.128	0.150
61	Sente seguro para jogar em diversas aplicações	2.19	0.701	0.083

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 22 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 2

Item	Cruzamento	χ^2	sig	V
11	Terceiros utilizam os dados	6.75	0.150	0.146
12	Aceita termos de aceitação	4.33	0.363	0.117

Grupo 3

Item	Cruzamento	χ^2	sig	V
15	Confia a partilha de informação	-	-	0.080
16	Utilização do mesmo tem risco aos dados móveis	-	-	0.119

17	Utilização da câmara tem risco de segurança	-	-	0.120
18	Instalar uma aplicação para manter a privacidade	-	-	0.121

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	1.26	0.869	0.063
26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	-	-	0.085

Grupo 7

Item	Cruzamento	χ^2	sig	V
40	Considera útil ter possibilidade de partilhar multimédia	-	-	0.104

Grupo 9

Item	Cruzamento	χ^2	sig	V
55	Costuma usar <i>Smartphone</i> para partilhar multimédia	-	-	0.110
56	Monitorizar atividade física/desportiva	3.56	0.469	0.106
57	Usa GPS para atividades físicas e desportivas	5.70	0.223	0.134

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	4.24	0.374	0.116
59	Considera seguro de partilhar multimédia	-	-	0.169*
60	Sente seguro para comunicar-se com contactos e empresa	-	-	0.138**
61	Sente seguro para jogar em diversas aplicações	-	-	0.132

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 23 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Grupo 2

Item	Cruzamento	χ^2	sig	V
11	Terceiros utilizam os dados	2.38	0.132	0.087
12	Aceita termos de aceitação	8.06	0.006	0.159*

Grupo 3

Item	Cruzamento	χ^2	sig	V
------	------------	----------	-----	---

14	Utilização de aplicações tem risco	5.74	0.219	0.135
17	Utilização da câmara tem risco de segurança	5.11	0.276	0.127
18	Instalar uma aplicação para manter a privacidade	8.77	0.067	0.166**

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	4.76	0.030	0.122*
22	Sempre teve certeza como era a utilização do <i>Smartphone</i>	4.68	0.035	0.121*
23	Confia no <i>Smartphone</i>	6.52	0.014	0.143*
24	Sente-se confortável ao usar o <i>Smartphone</i>	3.55	0.067	0.106**
26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	2.78	0.113	0.094

Grupo 8

Item	Cruzamento	χ^2	sig	V
48	Necessidade de tapar a câmara do <i>Smartphone</i>	28.10	0.001	0.298*
49	Necessidade de desligar o GPS	0.36	0.626	0.034
50	Desligar o <i>Smartphone</i> no momento que não utiliza	4.61	0.039	0.121*
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.52	0.142	0.089
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	1.99	0.181	0.079

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	1.78	0.211	0.075
59	Considera seguro de partilhar multimédia	6.56	0.161	0.144
60	Sente seguro para comunicar-se com contactos e empresa	6.46	0.167	0.143
61	Sente seguro para jogar em diversas aplicações	6.95	0.139	0.148

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 24 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes

Sexo	I.C
------	-----

tem	Cruzamento	O.R	Inferior	Superior
12	Aceita termos de aceitação	2,12*	1,26	3,58
19	Houve alturas que se preocupou com a privacidade	0,50*	0,27	0,94
22	Sempre teve certeza como era a utilização do <i>Smartphone</i>	1,70*	1,05	2,75
23	Confia no <i>Smartphone</i>	2,09*	1,18	3,70
48	Necessidade tapar a câmara em algumas situações	0,26*	0,16	0,43
50	Desligar o <i>Smartphone</i> no momento que não utiliza	3,57*	1,04	12,27

Nota: * Significativo ao nível de 5% ($\alpha=0.05$); O.R: *Odds Ratio*; I.C: Intervalo de Confiança

Tabela 25 - Razão de chance (*Odds Ratio*) por Sexo dos estudantes

Grupo 2				
Item	Cruzamento	χ^2	sig	V
11	Terceiros utilizam os dados	3.75	0.061	0.109*
12	Aceita termos de aceitação	0.46	0.589	0.038
Grupo 3				
Item	Cruzamento	χ^2	sig	V
14	Utilização de aplicações tem risco	3.97	0.410	0.112
17	Utilização da câmara tem risco de segurança	12.99	0.011	0.202*
18	Instalar uma aplicação para manter a privacidade	11.38	0.023	0.189*
Grupo 4				
Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	0.74	0.399	0.048
22	Sempre teve certeza de como era a utilização do <i>Smartphone</i>	0,69	0,468	0,047
23	Confia no <i>Smartphone</i>	0,27	0,657	0,029
24	Sente-se confortável ao usar o <i>Smartphone</i>	0,30	0,795	0,031
26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	3.89	0.059	0.111**
Grupo 8				
Item	Cruzamento	χ^2	sig	V
48	Necessidade de tapar a câmara do <i>Smartphone</i>	0.00	1.000	0.002
49	Necessidade de desligar o GPS	0.05	0.905	0.013

50	Desligar o <i>Smartphone</i> no momento que não utiliza	1.12	0.278	0.061
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	0.23	0.635	0.027
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	0.11	0.812	0.019

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	0.79	0.395	0.050
59	Considera seguro de partilhar multimédia	0.63	0.960	0.044
60	Sente seguro para comunicar-se com contactos e empresa	7.14	0.128	0.150
61	Sente seguro para jogar em diversas aplicações	2.19	0.701	0.083

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 26 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 2

Item	Cruzamento	χ^2	sig	V
11	Terceiros utilizam os dados	6.75	0.150	0.146
12	Aceita termos de aceitação	4.33	0.363	0.117

Grupo 3

Item	Cruzamento	χ^2	sig	V
14	Utilização de aplicações tem risco	-	-	0.082
17	Utilização da câmara tem risco de segurança	-	-	0.120
18	Instalar uma aplicação para manter a privacidade	-	-	0.121

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	1.26	0.869	0.063
22	Sempre teve certeza de como era a utilização do <i>Smartphone</i>	11,16	0,025	0,188*
23	Confia no <i>Smartphone</i>	3,98	0,409	0,112
24	Sente-se confortável ao usar o <i>Smartphone</i>	-	-	0,186*

26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	-	-	0.085
----	---	---	---	-------

Grupo 8

Item	Cruzamento	χ^2	sig	V
48	Necessidade de tapar a câmara do <i>Smartphone</i>	4.37	0.358	0.117
49	Necessidade de desligar o GPS	3.12	0.538	0.099
50	Desligar o <i>Smartphone</i> no momento que não utiliza	-	-	0.088
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.32	0.678	0.085
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	5.40	0.248	0.131

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	4.24	0.374	0.116
59	Considera seguro de partilhar multimédia	-	-	0.169*
60	Sente seguro para comunicar-se com contactos e empresa	-	-	0.138**
61	Sente seguro para jogar em diversas aplicações	-	-	0.132

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 27 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Grupo 4

Item	Cruzamento	χ^2	sig	V
21	As funcionalidades não são consistentes como esperava	1.00	0.338	0.056
22	Sempre teve certeza como era a utilização do <i>Smartphone</i>	4.68	0.035	0.121*

Grupo 5

Item	Cruzamento	χ^2	sig	V
27	Utiliza <i>Smartphone</i> para uso académico	4.21	0.042	0.115*

Grupo 6

Item	Cruzamento	χ^2	sig	V
34	Considera fácil comunicar-se com seus contactos	-	-	0.150

35	As ferramentas do <i>Smartphone</i> são flexíveis	2.89	0.136	0.095**
36	Considera fácil compartilhar multimídias	-	-	0.114
37	Interação com <i>Smartphone</i> é flexível	-	-	0.103

Grupo 7

Item	Cruzamento	χ^2	sig	V
38	<i>Smartphone</i> é útil para comunicar (contactos pessoais)	-	-	0.132
39	<i>Smartphone</i> útil para comunicar (contactos universitários)	-	-	0.132
40	Considera útil ter possibilidade de partilhar multimídia	-	-	0.103
41	Usar ferramentas do <i>Smartphone</i> o trabalho fica rápido	4.94	0.035	0.125*
42	Usar <i>smartphone</i> aumenta a eficiência do trabalho	0.27	0.644	0.029
43	<i>Smartphone</i> afeta os estudos	7.92	0.095	0.158**
44	Usar <i>Smartphone</i> iria ser útil nos estudos	4.87	0.300	0.124

Grupo 8

Item	Cruzamento	χ^2	sig	V
45	Quer utilizar <i>Smartphone</i>	4.05	0.053	0.113*
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	15.58	0.001	0.222*

Grupo 9

Item	Cruzamento	χ^2	sig	V
55	Costuma usar <i>Smartphone</i> para partilhar multimídia	4.81	0.027	0.123*
56	Monitorizar atividade física/desportiva	0.98	0.334	0.056
57	Usa GPS para atividades físicas e desportivas	5.42	0.024	0.131*

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 28 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes

Sexo		I.C		
Item	Cruzamento	O.R	Inferior	Superior
22	Sempre teve certeza como era a utilização do <i>Smartphone</i>	1.70*	1.05	2.75
27	Utiliza <i>Smartphone</i> para uso académico	0.15	0.02	1.19

35	As ferramentas do <i>Smartphone</i> são flexíveis	0.35	0.10	1.23
41	Usar ferramentas do <i>Smartphone</i> o trabalho fica rápido	0.31*	0.11	0.92
45	Quer utilizar <i>Smartphone</i>	0.58*	0.34	0.99
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	2.63*	1.62	4.27
55	Costuma usar <i>Smartphone</i> para partilhar multimédia	0.22*	0.05	0.96
57	Usa GPS para atividades físicas e desportivas	1.83*	1.10	3.06

Nota: *Significativo ao nível de 5% ($\alpha = 0.05$); O.R: *Odds Ratio*; I.C: Intervalo de Confiança

Tabela 29 - Razão de chance (*Odds Ratio*) por Sexo dos estudantes

Grupo 4				
Item	Cruzamento	χ^2	sig	V
21	As funcionalidades não são consistentes como esperava	1.20	0.293	0.062
22	Sempre teve certeza de como era a utilização do <i>Smartphone</i>	0.69	0.468	0.047
Grupo 5				
Item	Cruzamento	χ^2	sig	V
27	Utiliza <i>Smartphone</i> para uso académico	1.32	0.265	0.064
Grupo 6				
Item	Cruzamento	χ^2	sig	V
34	Considera fácil comunicar-se com seus contactos	-	-	0.064
35	As ferramentas do <i>Smartphone</i> são flexíveis	0.18	0.810	0.024
36	Considera fácil partilhar multimídias	-	-	0.084
37	Interação com <i>Smartphone</i> é flexível	-	-	0.062
Grupo 7				
Item	Cruzamento	χ^2	sig	V
38	<i>Smartphone</i> é útil para comunicar (contactos pessoais)	-	-	0.125
39	<i>Smartphone</i> útil para comunicar (contactos universitários)	-	-	0.082
40	Considera útil ter possibilidade de partilhar multimédia	-	-	0.169

41	Usar ferramentas do smartphone o trabalho fica rápido	0.07	0.840	0.015
42	Usar <i>Smartphone</i> aumenta a eficiência do trabalho	1.72	0.225	0.074
43	<i>Smartphone</i> afeta os estudos	7.66	0.105	0.155
44	Usar <i>Smartphone</i> iria ser útil nos estudos	2.78	0.595	0.094

Grupo 8

Item	Cruzamento	χ^2	sig	V
45	Quer utilizar <i>Smartphone</i>	0.03	0.900	0.009
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	4.24	0.046	0.116*

Grupo 9

Item	Cruzamento	χ^2	sig	V
55	Costuma usar <i>Smartphone</i> para partilhar multimédia	0.81	0.470	0.051
56	Monitorizar atividade física/desportiva	1.49	0.238	0.069
57	Usa GPS para atividades físicas e desportivas	3.47	0.069	0.105**

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 30 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 4

Item	Cruzamento	χ^2	sig	V
21	As funcionalidades não são consistentes como esperava	2.28	0.685	0.085
22	Sempre teve certeza de como era a utilização do <i>Smartphone</i>	11.16	0.025	0.188*

Grupo 5

Item	Cruzamento	χ^2	sig	V
27	Utiliza <i>Smartphone</i> para uso académico	-	-	0.052

Grupo 6

Item	Cruzamento	χ^2	sig	V
34	Considera fácil comunicar-se com seus contactos	-	-	0.064
35	As ferramentas do <i>Smartphone</i> são flexíveis	0.18	0.810	0.024
36	Considera fácil partilhar multimídias	-	-	0.084

37	Interação com <i>Smartphone</i> é flexível	-	-	0.062
----	--	---	---	-------

Grupo 7

Item	Cruzamento	χ^2	sig	V
38	<i>Smartphone</i> é útil para comunicar (contactos pessoais)	-	-	0.132
39	<i>Smartphone</i> útil para comunicar (contactos universitários)	-	-	0.133
40	Considera útil ter possibilidade de partilhar multimédia	-	-	0.104
41	Usar ferramentas do <i>Smartphone</i> o trabalho fica rápido	3.28	0.511	0.102
42	Usar <i>Smartphone</i> aumenta a eficiência do trabalho	0.49	0.975	0.039
43	<i>Smartphone</i> afeta os estudos	-	-	0.136
44	Usar <i>Smartphone</i> iria ser útil nos estudos	-	-	0.114

Grupo 8

Item	Cruzamento	χ^2	sig	V
45	Quer utilizar <i>Smartphone</i>	4.78	0.310	0.123
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	7.53	0.110	0.154

Grupo 9

Item	Cruzamento	χ^2	sig	V
55	Costuma usar <i>Smartphone</i> para partilhar multimédia	-	-	0.110
56	Monitorizar atividade física/desportiva	3.56	0.469	0.106
57	Usa GPS para atividades físicas e desportivas	5.70	0.223	0.134

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 31 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Grupo 7

Item	Cruzamento	χ^2	sig	V
41	Usar ferramentas do <i>Smartphone</i> o trabalho fica rápido	4.94	0.035	0.125*
42	Usar <i>Smartphone</i> aumenta a eficiência do trabalho	0.27	0.644	0.029
43	<i>Smartphone</i> afeta os estudos	7.92	0.095	0.158**
44	Usar <i>Smartphone</i> iria ser útil nos estudos	4.87	0.300	0.124

Grupo 8

Item	Cruzamento	χ^2	sig	V
------	------------	----------	-----	---

45	Quer utilizar <i>Smartphone</i>	4.05	0.053	0.113*
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	15.58	0.001	0.222*
47	Adorava ter novas ferramentas no <i>Smartphone</i>	10.77	0.002	0.184*

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 32 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes

Sexo		I.C		
Item	Cruzamento	O.R	Inferior	Superior
41	Usar Ferramentas <i>Smartphone</i> , trabalho fica mais rápido	0,31	0,11	0,92
45	Quer utilizar <i>Smartphone</i>	0,58	0,34	0,99
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	2,63	1,62	4,27
47	Adorava ter novas ferramentas no <i>Smartphone</i>	2,57	1,45	4,57

Nota: O.R: *Odds Ratio*; I.C: Intervalo de Confiança

Tabela 33 – Razão de chance (*Odds Ratio*) por Sexo dos estudantes

Grupo 7				
Item	Cruzamento	χ^2	sig	V
41	Usar ferramentas do <i>Smartphone</i> o trabalho fica rápido	0.07	0.840	0.015
42	Usar <i>Smartphone</i> aumenta a eficiência do trabalho	1.72	0.225	0.074
43	<i>Smartphone</i> afeta os estudos	7.66	0.105	0.155
44	Usar <i>Smartphone</i> iria ser útil nos estudos	2.78	0.595	0.094

Grupo 8				
Item	Cruzamento	χ^2	sig	V
45	Quer utilizar <i>Smartphone</i>	0.03	0.900	0.009
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	4.24	0.046	0.116*
47	Adorava ter novas ferramentas no <i>Smartphone</i>	0.17	0.765	0.023

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 34 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 7				
Item	Cruzamento	χ^2	sig	V
41	Usar ferramentas do <i>Smartphone</i> o trabalho fica rápido	3.28	0.511	0.102
42	Usar <i>Smartphone</i> aumenta a eficiência do trabalho	0.49	0.975	0.039
43	<i>Smartphone</i> afeta os estudos	-	-	0.136
44	Usar <i>Smartphone</i> iria ser útil nos estudos	-	-	0.114

Grupo 8				
Item	Cruzamento	χ^2	sig	V
45	Quer utilizar <i>Smartphone</i>	4.78	0.310	0.123
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	7.53	0.110	0.154
47	Adorava ter novas ferramentas no <i>Smartphone</i>	1.60	0.810	0.071

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 35 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Grupo 4				
Item	Cruzamento	χ^2	sig	V
21	As funcionalidades não são consistentes como esperava	1.00	0.338	0.056
22	Sempre teve certeza de como era a utilização do <i>Smartphone</i>	4.68	0.035	0.121*
25	Utiliza bem o <i>Smartphone</i>	0.31	0.682	0.031

Grupo 5				
Item	Cruzamento	χ^2	sig	V
27	Utiliza <i>Smartphone</i> para uso académico	4.21	0.042	0.115*

Grupo 6				
Item	Cruzamento	χ^2	sig	V
32	É fácil aprender a utilizar <i>Smartphone</i>	-	-	0.135
33	Utilização de <i>Smartphone</i> não requer esforço mental	3.45	0.486	0.104
34	Considera fácil comunicar-se com seus contactos	-	-	0.150

35	As ferramentas do <i>Smartphone</i> são flexíveis	2.89	0.136	0.095**
36	Considera fácil compartilhar multimídias	-	-	0.114
37	Interação com <i>Smartphone</i> é flexível	-	-	0.103

Grupo 7

Item	Cruzamento	χ^2	sig	V
38	<i>Smartphone</i> é útil para comunicar (contactos pessoais)	-	-	0.132
39	<i>Smartphone</i> útil para comunicar (contactos universitários)	-	-	0.132
40	Considera útil ter possibilidade de partilhar multimídia	-	-	0.103
41	Usar ferramentas do <i>Smartphone</i> o trabalho fica rápido	4.94	0.035	0.125*
42	Usar <i>Smartphone</i> aumenta a eficiência do trabalho	0.27	0.644	0.029
43	<i>Smartphone</i> afeta os estudos	7.92	0.095	0.158**
44	Usar <i>Smartphone</i> iria ser útil nos estudos	4.87	0.300	0.124

Grupo 8

Item	Cruzamento	χ^2	sig	V
45	Quer utilizar <i>Smartphone</i>	4.05	0.053	0.113*

Grupo 9

Item	Cruzamento	χ^2	sig	V
56	Monitorizar atividade física/desportiva	0.98	0.334	0.056
57	Usa GPS para atividades físicas e desportivas	5.42	0.024	0.131*
Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	1.78	0.211	0.075
59	Considera seguro de compartilhar multimídia	6.56	0.161	0.144
60	Sente seguro para comunicar-se com contactos e empresa	6.46	0.167	0.143
61	Sente seguro para jogar em diversas aplicações	6.95	0.139	0.148

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 36 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes

Sexo		I.C		
Item	Cruzamento	O.R	Inferior	Superior

41	Usar ferramentas do <i>Smartphone</i> o trabalho fica rápido	0.31*	0.11	0.92
45	Quer utilizar <i>Smartphone</i>	0.58*	0.34	0.99
57	Usa GPS para atividades físicas e desportivas	1.83*	1.10	3.06

Nota: *Significativo ao nível de 5% ($\alpha = 0.05$); O.R: *Odds Ratio*; I.C: Intervalo de Confiança

Tabela 37 - Razão de chance (Odds Ratio) por Sexo dos estudantes

Grupo 9				
Item	Cruzamento	χ^2	sig	V
57	Usa GPS para atividades físicas e desportivas	3.47	0.069	0.105**

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 38 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 4				
Item	Cruzamento	χ^2	sig	V
21	As funcionalidades não são consistentes como esperava	2.28	0.685	0.085
22	Sempre teve certeza de como era a utilização do <i>Smartphone</i>	11.16	0.025	0.188
25	Utiliza bem o <i>Smartphone</i>	-	-	0.078

Grupo 5				
Item	Cruzamento	χ^2	sig	V
27	Utiliza <i>Smartphone</i> para uso académico	-	-	0.052

Grupo 6				
Item	Cruzamento	χ^2	sig	V
32	É fácil aprender a utilizar <i>Smartphone</i>	-	-	0.125
33	Utilização de <i>Smartphone</i> não requer esforço mental	-	-	0.124
34	Considera fácil comunicar-se com seus contactos	-	-	0.128
35	As ferramentas do <i>Smartphone</i> são flexíveis	-	-	0.129
36	Considera fácil partilhar multimídias	-	-	0.149*

37	Interação com <i>Smartphone</i> é flexível	-	-	0.120
Grupo 7				
Item	Cruzamento	χ^2	<i>sig</i>	V
38	Smartphone é útil para comunicar (contactos pessoais)	-	-	0.132
39	<i>Smartphone</i> útil para comunicar (contactos universitários)	-	-	0.133
40	Considera útil ter possibilidade de partilhar multimídia	-	-	0.104
41	Usar ferramentas do <i>Smartphone</i> o trabalho fica rápido	3.28	0.511	0.102
42	Usar <i>Smartphone</i> aumenta a eficiência do trabalho	0.49	0.975	0.039
43	<i>Smartphone</i> afeta os estudos	-	-	0.136
44	Usar <i>Smartphone</i> iria ser útil nos estudos	-	-	0.114
Grupo 8				
Item	Cruzamento	χ^2	<i>sig</i>	V
45	Quer utilizar <i>Smartphone</i>	4.78	0.310	0.123
50	Desligar o <i>Smartphone</i> no momento que não utiliza	-	-	0.088
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.32	0.678	0.085
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	5.40	0.248	0.131
Grupo 9				
Item	Cruzamento	χ^2	<i>sig</i>	V
56	Monitorizar atividade física/desportiva	3.56	0.469	0.106
57	Usa GPS para atividades físicas e desportivas	5.70	0.223	0.134
Grupo 10				
Item	Cruzamento	χ^2	<i>sig</i>	V
58	Divulga informações pessoais no <i>Smartphone</i>	4.24	0.374	0.116
59	Considera seguro de partilhar multimídia	-	-	0.169*
60	Sente seguro para comunicar-se com contactos e empresa	-	-	0.138**
61	Sente seguro para jogar em diversas aplicações	-	-	0.132

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 39 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Grupo 4				
Item	Cruzamento	χ^2	sig	V
21	As funcionalidades não são consistentes como esperava	1.00	0.338	0.056
22	Sempre teve certeza de como era a utilização do <i>Smartphone</i>	4.68	0.035	0.121*
25	Utiliza bem o <i>Smartphone</i>	0.31	0.682	0.031
Grupo 5				
Item	Cruzamento	χ^2	sig	V
27	Utiliza <i>Smartphone</i> para uso académico	4.21	0.042	0.115*
Grupo 6				
Item	Cruzamento	χ^2	sig	V
32	É fácil aprender a utilizar <i>Smartphone</i>	-	-	0.135
33	Utilização de <i>Smartphone</i> não requer esforço mental	3.45	0.486	0.104
34	Considera fácil comunicar-se com seus contactos	-	-	0.150**
35	As ferramentas do <i>Smartphone</i> são flexíveis	2.89	0.136	0.095**
36	Considera fácil partilhar multimídias	-	-	0.114
37	Interação com <i>Smartphone</i> é flexível	-	-	0.103
Grupo 7				
Item	Cruzamento	χ^2	sig	V
38	<i>Smartphone</i> é útil para comunicar (contactos pessoais)	-	-	0.132
39	<i>Smartphone</i> útil para comunicar (contactos universitários)	-	-	0.132
40	Considera útil ter possibilidade de partilhar multimídia	-	-	0.103
41	Usar ferramentas do <i>Smartphone</i> o trabalho fica rápido	4.94	0.035	0.125*
42	Usar <i>Smartphone</i> aumenta a eficiência do trabalho	0.27	0.644	0.029
43	<i>Smartphone</i> afeta os estudos	7.92	0.095	0.158**
44	Usar <i>Smartphone</i> iria ser útil nos estudos	4.87	0.300	0.124
Grupo 8				
Item	Cruzamento	χ^2	sig	V
45	Quer utilizar <i>Smartphone</i>	4.05	0.053	0.113*
50	Desligar o <i>Smartphone</i> no momento que não utiliza	4.61	0.039	0.121*
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.52	0.142	0.089

52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	1.99	0.181	0.079
----	--	------	-------	-------

Grupo 9

Item	Cruzamento	χ^2	sig	V
56	Monitorizar atividade física/desportiva	0.98	0.334	0.056
57	Usa GPS para atividades físicas e desportivas	5.42	0.024	0.131*

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 40 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes

Sexo		I.C		
Item	Cruzamento	O.R	Inferior	Superior
12	Aceita termos de aceitação	2,12	1,26	3,58
48	Necessidade tapar a câmara em algumas situações	0,26	0,16	0,43
50	Desligar o <i>Smartphone</i> no momento que não utiliza	3,57	1,04	12,27
55	Costuma usar <i>Smartphone</i> para partilhar multimédia	0,22	0,05	0,96
57	Usa GPS para atividades físicas e desportivas	1,83	1,10	3,06

Nota: O.R: *Odds Ratio*; I.C: Intervalo de Confiança

Tabela 41 - Razão de chance (Odds Ratio) por Sexo dos estudantes

Grupo 3

Item	Cruzamento	χ^2	sig	V
15	Confia a partilha de informação	10,77	0,029	0.184*
17	Utilização da câmara tem risco de segurança	12,99	0,011	0.202*
18	Instalar uma aplicação para manter a privacidade	11,38	0,023	0.189*

Grupo 9

Item	Cruzamento	χ^2	sig	V
57	Usa GPS para atividades físicas e desportivas	3,468	0,069	0.105**

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 42 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 2				
Item	Cruzamento	χ^2	sig	V
12	Aceita termos de aceitação	4.33	0.363	0.117

Grupo 3				
Item	Cruzamento	χ^2	sig	V
15	Confia a partilha de informação	-	-	0.080
16	Utilização do mesmo tem risco aos dados móveis	-	-	0.119
17	Utilização da câmara tem risco de segurança	-	-	0.120
18	Instalar uma aplicação para manter a privacidade	-	-	0.121

Grupo 8				
Item	Cruzamento	χ^2	sig	V
48	Necessidade de tapar a câmara do <i>Smartphone</i>	4.37	0.358	0.117
49	Necessidade de desligar o GPS	3.12	0.538	0.099
50	Desligar o <i>Smartphone</i> no momento que não utiliza	-	-	0.088
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.32	0.678	0.085
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	5.40	0.248	0.131

Grupo 9				
Item	Cruzamento	χ^2	sig	V
55	Costuma usar <i>Smartphone</i> para partilhar multimédia	-	-	0.110
56	Monitorizar atividade física/desportiva	3.56	0.469	0.106
57	Usa GPS para atividades físicas e desportivas	5.70	0.223	0.134

Grupo 10				
Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	4.24	0.374	0.116
59	Considera seguro de partilhar multimédia	-	-	0.169*
60	Sente seguro para comunicar-se com contactos e empresa	-	-	0.138**
61	Sente seguro para jogar em diversas aplicações	-	-	0.132

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 43 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Grupo 2				
Item	Cruzamento	χ^2	sig	V
11	Terceiros utilizam os dados	2.38	0.132	0.087
12	Aceita termos de aceitação	8.06	0.006	0.159*
Grupo 3				
Item	Cruzamento	χ^2	sig	V
14	Utilização de aplicações tem risco	5.74	0.219	0.135
15	Confia a partilha de informação	9.07	0.059	0.169**
16	Utilização do mesmo tem risco aos dados móveis	8.47	0.076	0.163**
17	Utilização da câmara tem risco de segurança	5.11	0.276	0.127
18	Instalar uma aplicação para manter a privacidade	8.77	0.067	0.166**
Grupo 4				
Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	4.76	0.030	0.122*
23	Confia no <i>Smartphone</i>	6.52	0.014	0.143*
24	Sente-se confortável ao usar o <i>Smartphone</i>	3.55	0.067	0.106**
26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	2.78	0.113	0.094
Grupo 8				
Item	Cruzamento	χ^2	sig	V
48	Necessidade de tapar a câmara do <i>Smartphone</i>	28.10	0.001	0.298*
49	Necessidade de desligar o GPS	0.36	0.626	0.034
50	Desligar o <i>Smartphone</i> no momento que não utiliza	4.61	0.039	0.121*
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.54	0.142	0.089
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	1.99	0.181	0.079
Grupo 10				
Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	1.78	0.211	0.075
59	Considera seguro de partilhar multimédia	6.56	0.161	0.144
60	Sente seguro para comunicar-se com contactos e empresa	6.46	0.167	0.143
61	Sente seguro para jogar em diversas aplicações	6.95	0.139	0.148

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 44 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes

Sexo			I.C	
Ite m	Cruzamento	O.R	Inferio r	Superio r
12	Aceita termos de aceitação	2,12*	1,26	3,58
19	Houve alturas que se preocupou com a privacidade	0,50*	0,27	0,94
23	Confia no <i>Smartphone</i>	2,09*	1,18	3,70
48	Necessidade tapar a câmara em algumas situações	0,26*	0,16	0,43
50	Desligar o <i>Smartphone</i> no momento que não utiliza	3,57*	1,04	12,27

Nota: O.R: *Odds Ratio*; I.C: Intervalo de Confiança

Tabela 45 - Razão de chance (Odds Ratio) por Sexo dos estudantes

Grupo 2				
Item	Cruzamento	χ^2	sig	V
11	Terceiros utilizam os dados	3.75	0.061	0.109*
12	Aceita termos de aceitação	0.46	0.589	0.038
Grupo 3				
Item	Cruzamento	χ^2	sig	V
14	Utilização de aplicações tem risco	3.97	0.410	0.112
15	Confia a partilha de informação	10.77	0.029	0.184*
16	Utilização do mesmo tem risco aos dados móveis	4.24	0.375	0.116
17	Utilização da câmara tem risco de segurança	12.99	0.011	0.202*
18	Instalar uma aplicação para manter a privacidade	11.38	0.023	0.189*
Grupo 4				
Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	0.74	0.399	0.048
23	Confia no <i>Smartphone</i>	0.27	0.657	0.029
24	Sente-se confortável ao usar o <i>Smartphone</i>	0.30	0.795	0.031

26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	3.89	0.059	0.111*
----	---	------	-------	--------

Grupo 8

Item	Cruzamento	χ^2	sig	V
48	Necessidade de tapar a câmara do <i>Smartphone</i>	0.00	1.000	0.002
49	Necessidade de desligar o GPS	0.05	0.905	0.013
50	Desligar o <i>Smartphone</i> no momento que não utiliza	1.12	0.278	0.061
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	0.23	0.635	0.027
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	0.11	0.812	0.019

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	0.79	0.395	0.050
59	Considera seguro de partilhar multimédia	0.63	0.960	0.044
60	Sente seguro para comunicar-se com contactos e empresa	7.14	0.128	0.150
61	Sente seguro para jogar em diversas aplicações	2.19	0.701	0.083

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 46 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 2

Item	Cruzamento	χ^2	sig	V
11	Terceiros utilizam os dados	6.75	0.150	0.146
12	Aceita termos de aceitação	4.33	0.363	0.117

Grupo 3

Item	Cruzamento	χ^2	sig	V
14	Utilização de aplicações tem risco	-	-	0.082
15	Confia a partilha de informação	-	-	0.080
16	Utilização do mesmo tem risco aos dados móveis	-	-	0.119
17	Utilização da câmara tem risco de segurança	-	-	0.120
18	Instalar uma aplicação para manter a privacidade	-	-	0.121

Grupo 4				
Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	1.26	0.869	0.063
23	Confia no <i>Smartphone</i>	3.98	0.409	0.112
24	Sente-se confortável ao usar o <i>Smartphone</i>	-	-	0.186*
26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	-	-	0.085

Grupo 8				
Item	Cruzamento	χ^2	sig	V
48	Necessidade de tapar a câmara do <i>Smartphone</i>	4.37	0.358	0.117
49	Necessidade de desligar o GPS	3.12	0.538	0.099
50	Desligar o smartphone no momento que não utiliza	-	-	0.088
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.32	0.678	0.085
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	5.40	0.248	0.131

Grupo 10				
Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	4.24	0.374	0.116
59	Considera seguro de partilhar multimédia	-	-	0.169*
60	Sente seguro para comunicar-se com contactos e empresa	-	-	0.138**
61	Sente seguro para jogar em diversas aplicações	-	-	0.132

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 47 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Grupo 4				
Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	4.76	0.030	0.122*
20	Não comprava um <i>Smartphone</i> se voltasse atrás	3.25	0.112	0.101**
23	Confia no <i>Smartphone</i>	6.52	0.014	0.143*
24	Sente-se confortável ao usar o <i>Smartphone</i>	3.55	0.067	0.106**

26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	2.78	0.113	0.094**
----	---	------	-------	---------

Grupo 8

Item	Cruzamento	χ^2	sig	V
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	15.58	0.001	0.222*
47	Adorava ter novas ferramentas no <i>Smartphone</i>	10.77	0.002	0.184*
48	Necessidade de tapar a câmara do <i>Smartphone</i>	28.10	0.001	0.298*
49	Necessidade de desligar o GPS	0.36	0.626	0.034
50	Desligar o <i>Smartphone</i> no momento que não utiliza	4.61	0.039	0.121*
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.52	0.142	0.089
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	1.99	0.181	0.079

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 48 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes

Sexo			I.C	
Ite m	Cruzamento	O.R	Inferio r	Superio r
19	Houve alturas que se preocupou com a privacidade	0,50*	0,27	0,94
23	Confia no <i>Smartphone</i>	2,09*	1,18	3,70
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	2,63*	1,62	4,27
47	Adorava ter novas ferramentas no <i>Smartphone</i>	2,57*	1,45	4,57
48	Necessidade tapar a câmara em algumas situações	0,26*	0,16	0,43
50	Desligar o <i>Smartphone</i> no momento que não utiliza	3,57*	1,04	12,27

Nota: O.R: Odds Ratio; I.C: Intervalo de Confiança

Tabela 49 - Razão de chance (Odds Ratio) por Sexo dos estudantes

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	0.74	0.399	0.048
20	Não comprava um <i>Smartphone</i> se voltasse atrás	0.20	0.761	0.025

23	Confia no <i>Smartphone</i>	0.27	0.657	0.029
24	Sente-se confortável ao usar o <i>Smartphone</i>	0.30	0.795	0.031
26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	3.89	0.059	0.111**

Grupo 8

Item	Cruzamento	χ^2	sig	V
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	4.24	0.046	0.116*
47	Adorava ter novas ferramentas no <i>Smartphone</i>	0.17	0.765	0.023
48	Necessidade de tapar a câmara do <i>Smartphone</i>	0.00	1.000	0.002
49	Necessidade de desligar o GPS	0.05	0.905	0.013
50	Desligar o <i>Smartphone</i> no momento que não utiliza	1.12	0.278	0.061
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	0.23	0.635	0.027
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	0.11	0.812	0.019

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 50 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 4

Item	Cruzamento	χ^2	sig	V
24	Sente-se confortável ao usar o <i>Smartphone</i>	-	-	0.186*

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 51 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	4.76	0.030	0.122*
23	Confia no <i>Smartphone</i>	6.52	0.014	0.143*
24	Sente-se confortável ao usar o <i>Smartphone</i>	3.55	0.067	0.106**

25	Utiliza bem o <i>Smartphone</i>	0.31	0.682	0.031
Grupo 5				
Item	Cruzamento	χ^2	sig	V
27	Utiliza <i>Smartphone</i> para uso académico	4.21	0.042	0.115*
Grupo 6				
Item	Cruzamento	χ^2	sig	V
32	É fácil aprender a utilizar <i>Smartphone</i>	-	-	0.135
33	Utilização de <i>Smartphone</i> não requer esforço mental	3.49	0.486	0.104
34	Considera fácil comunicar-se com seus contactos	-	-	0.150**
35	As ferramentas do <i>Smartphone</i> são flexíveis	2.89	0.136	0.095**
36	Considera fácil partilhar multimídias	-	-	0.114
37	Interação com <i>Smartphone</i> é flexível	-	-	0.103
Grupo 7				
Item	Cruzamento	χ^2	sig	V
38	<i>Smartphone</i> é útil para comunicar (contactos pessoais)	-	-	0.132
39	<i>Smartphone</i> útil para comunicar (contactos universitários)	-	-	0.132
40	Considera útil ter possibilidade de partilhar multimídia	-	-	0.103
41	Usar ferramentas do <i>Smartphone</i> o trabalho fica rápido	4.94	0.035	0.125*
42	Usar <i>Smartphone</i> aumenta a eficiência do trabalho	0.27	0.644	0.029
43	<i>Smartphone</i> afeta os estudos	7.92	0.095	0.158**
44	Usar <i>smartphone</i> iria ser útil nos estudos	4.87	0.300	0.124
Grupo 8				
Item	Cruzamento	χ^2	sig	V
45	Quer utilizar <i>Smartphone</i>	4.05	0.053	0.113*
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	15.58	0.001	0.222*
47	Adorava ter novas ferramentas no <i>Smartphone</i>	10.77	0.002	0.184*
48	Necessidade de tapar a câmara do <i>Smartphone</i>	28.10	0.001	0.298*
49	Necessidade de desligar o GPS	0.36	0.626	0.034
50	Desligar o <i>Smartphone</i> no momento que não utiliza	4.61	0.039	0.121*
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.52	0.142	0.089

52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	1.99	0.181	0.079
----	--	------	-------	-------

Grupo 9

Item	Cruzamento	χ^2	sig	V
55	Costuma usar <i>Smartphone</i> para partilhar multimídia	4.81	0.027	0.123*
56	Monitorizar atividade física/desportiva	0.98	0.334	0.056
57	Usa GPS para atividades físicas e desportivas	5.42	0.024	0.131*

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	1.78	0.211	0.075
59	Considera seguro de compartilhar multimídia	6.56	0.161	0.144
60	Sente seguro para comunicar-se com contactos e empresa	6.46	0.167	0.143
61	Sente seguro para jogar em diversas aplicações	6.95	0.139	0.148

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 52 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes

Item	Cruzamento	Sexo	I.C.	
			O.R	Inferior Superior
19	Houve alturas que se preocupou com a privacidade	0,50	0,27	0,94
23	Confia no <i>Smartphone</i>	2,09	1,18	3,70
41	Usar Ferramentas <i>Smartphone</i> , trabalho fica mais rápido	0,31	0,11	0,92
45	Quer utilizar <i>Smartphone</i>	0,58	0,34	0,99
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	2,63	1,62	4,27
47	Adorava ter novas ferramentas no <i>Smartphone</i>	2,57	1,45	4,57
48	Necessidade tapar a câmara em algumas situações	0,26	0,16	0,43
50	Desligar o <i>Smartphone</i> no momento que não utiliza	3,57	1,04	12,27
55	Costuma usar <i>Smartphone</i> para partilhar multimídia	0,22	0,05	0,96
57	Usa GPS para atividades físicas e desportivas	1,83	1,10	3,06

Nota: O.R: *Odds Ratio*; I.C: Intervalo de Confiança

Tabela 53 - Razão de chance (Odds Ratio) por Sexo dos estudantes

Grupo 4				
Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	0.74	0.399	0.048
23	Confia no <i>Smartphone</i>	0.27	0.657	0.029
24	Sente-se confortável ao usar o <i>Smartphone</i>	0.30	0.795	0.031
25	Utiliza bem o <i>Smartphone</i>	0.02	1.000	0.007
Grupo 5				
Item	Cruzamento	χ^2	sig	V
27	Utiliza <i>Smartphone</i> para uso académico	1.32	0.265	0.064
Grupo 6				
Item	Cruzamento	χ^2	sig	V
32	É fácil aprender a utilizar <i>Smartphone</i>	-	-	0.044
33	Utilização de <i>Smartphone</i> não requer esforço mental	3.10	0.555	0.098
34	Considera fácil comunicar-se com seus contactos	-	-	0.064
35	As ferramentas do <i>Smartphone</i> são flexíveis	0.18	0.810	0.024
36	Considera fácil partilhar multimídias	-	-	0.084
37	Interação com <i>Smartphone</i> é flexível	-	-	0.062
Grupo 7				
Item	Cruzamento	χ^2	sig	V
38	<i>Smartphone</i> é útil para comunicar (contactos pessoais)	-	-	0.125
39	<i>Smartphone</i> útil para comunicar (contactos universitários)	-	-	0.082
40	Considera útil ter possibilidade de partilhar multimídia	-	-	0.169
41	Usar ferramentas do <i>Smartphone</i> o trabalho fica rápido	0.07	0.840	0.015
42	Usar <i>Smartphone</i> aumenta a eficiência do trabalho	1.72	0.225	0.074
43	<i>Smartphone</i> afeta os estudos	7.66	0.105	0.155
44	Usar <i>Smartphone</i> iria ser útil nos estudos	2.78	0.595	0.094
Grupo 8				
Item	Cruzamento	χ^2	sig	V
45	Quer utilizar <i>Smartphone</i>	0.03	0.900	0.009
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	4.24	0.046	0.116*

47	Adorava ter novas ferramentas no <i>Smartphone</i>	0.17	0.765	0.023
48	Necessidade de tapar a câmara do <i>Smartphone</i>	0.00	1.000	0.002
49	Necessidade de desligar o GPS	0.05	0.905	0.013
50	Desligar o <i>Smartphone</i> no momento que não utiliza	1.12	0.278	0.061
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	0.23	0.635	0.027
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	0.11	0.812	0.019

Grupo 9

Item	Cruzamento	χ^2	sig	V
55	Costuma usar <i>Smartphone</i> para partilhar multimédia	0.81	0.470	0.051
56	Monitorizar atividade física/desportiva	1.49	0.238	0.069
57	Usa GPS para atividades físicas e desportivas	3.47	0.069	0.105**

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	0.79	0.395	0.050
59	Considera seguro de partilhar multimédia	0.63	0.960	0.044
60	Sente seguro para comunicar-se com contactos e empresa	7.14	0.128	0.150
61	Sente seguro para jogar em diversas aplicações	2.19	0.701	0.083

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 54 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	1.26	0.869	0.063
23	Confia no <i>Smartphone</i>	3.98	0.409	0.112
24	Sente-se confortável ao usar o <i>Smartphone</i>	-	-	0.186*
25	Utiliza bem o <i>Smartphone</i>	-	-	0.078

Grupo 5

Item	Cruzamento	χ^2	sig	V
27	Utiliza <i>Smartphone</i> para uso académico	-	-	0.052

Grupo 6

Item	Cruzamento	χ^2	sig	V
32	É fácil aprender a utilizar <i>Smartphone</i>	-	-	0.125
33	Utilização de <i>Smartphone</i> não requer esforço mental	-	-	0.124
34	Considera fácil comunicar-se com seus contactos	-	-	0.128
35	As ferramentas do <i>Smartphone</i> são flexíveis	-	-	0.129
36	Considera fácil partilhar multimídias	-	-	0.149*
37	Interação com <i>Smartphone</i> é flexível	-	-	0.120

Grupo 7

Item	Cruzamento	χ^2	sig	V
38	<i>Smartphone</i> é útil para comunicar (contactos pessoais)	-	-	0.132
39	<i>Smartphone</i> útil para comunicar (contactos universitários)	-	-	0.133
40	Considera útil ter possibilidade de partilhar multimídia	-	-	0.104
41	Usar ferramentas do <i>Smartphone</i> o trabalho fica rápido	3.28	0.511	0.102
42	Usar <i>Smartphone</i> aumenta a eficiência do trabalho	0.49	0.975	0.039
43	<i>Smartphone</i> afeta os estudos	-	-	0.136
44	Usar <i>Smartphone</i> iria ser útil nos estudos	-	-	0.114

Grupo 8

Item	Cruzamento	χ^2	sig	V
45	Quer utilizar <i>Smartphone</i>	4.78	0.310	0.123
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	7.53	0.110	0.154
47	Adorava ter novas ferramentas no <i>Smartphone</i>	1.60	0.810	0.071
48	Necessidade de tapar a câmara do <i>Smartphone</i>	4.37	0.358	0.117
49	Necessidade de desligar o GPS	3.12	0.538	0.099
50	Desligar o <i>Smartphone</i> no momento que não utiliza	-	-	0.088
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.32	0.678	0.085
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	5.40	0.248	0.131

Grupo 9

Item	Cruzamento	χ^2	sig	V
55	Costuma usar <i>Smartphone</i> para partilhar multimídia	-	-	0.110
56	Monitorizar atividade física/desportiva	3.56	0.469	0.106

57	Usa GPS para atividades físicas e desportivas	5.70	0.223	0.134
----	---	------	-------	-------

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	4.24	0.374	0.116
59	Considera seguro de compartilhar multimídia	-	-	0.169*
60	Sente seguro para comunicar-se com contactos e empresa	-	-	0.138**
61	Sente seguro para jogar em diversas aplicações	-	-	0.132

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 55 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	4.76	0.030	0.122*
20	Não comprava um <i>Smartphone</i> se voltasse atrás	3.25	0.112	0.101**
21	As funcionalidades não são consistentes como esperava	1.00	0.338	0.056
22	Sempre teve certeza de como era a utilização do <i>Smartphone</i>	4.68	0.035	0.121*
26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	2.78	0.113	0.094**

Grupo 8

Item	Cruzamento	χ^2	sig	V
45	Quer utilizar <i>Smartphone</i>	4.05	0.053	0.113*
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	15.58	0.001	0.222*
48	Necessidade de tapar a câmara do <i>Smartphone</i>	28.10	0.001	0.298*
49	Necessidade de desligar o GPS	0.36	0.626	0.034
50	Desligar o <i>Smartphone</i> no momento que não utiliza	4.61	0.039	0.121*
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.52	0.142	0.089
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	1.99	0.181	0.079

Grupo 10

Item	Cruzamento	χ^2	sig	V
------	------------	----------	-----	---

58	Divulga informações pessoais no <i>Smartphone</i>	1.78	0.211	0.075
59	Considera seguro de compartilhar multimídia	6.56	0.161	0.144
60	Sente seguro para comunicar-se com contactos e empresa	6.46	0.167	0.143
61	Sente seguro para jogar em diversas aplicações	6.95	0.139	0.148

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 56 - Teste Qui-quadrado de Independência e V de Crámer por Sexo dos estudantes

Sexo			I.C.	
Item	Cruzamento	O.R	Inferior	Superior
19	Houve alturas que se preocupou com a privacidade	0,50	0,27	0,94
22	Sempre teve certeza de como era a utilização do <i>Smartphone</i>	1,70	1,05	2,75
45	Quer utilizar <i>Smartphone</i>	0,58	0,34	0,99
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	2,63	1,62	4,27
48	Necessidade tapar a câmara em algumas situações	0,26	0,16	0,43
50	Desligar o <i>Smartphone</i> no momento que não utiliza	3,57	1,04	12,27

Nota: O.R: *Odds Ratio*; I.C: Intervalo de Confiança

Tabela 57 - Razão de chance (*Odds Ratio*) por Sexo dos estudantes

Grupo 4				
Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	0.74	0.399	0.048
20	Não comprava um <i>Smartphone</i> se voltasse atrás	0.20	0.761	0.025
21	As funcionalidades não são consistentes como esperava	1.20	0.293	0.062
22	Sempre teve certeza de como era a utilização do <i>Smartphone</i>	0.69	0.468	0.047
26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	3.89	0.059	0.111*

Grupo 8

Item	Cruzamento	χ^2	sig	V
------	------------	----------	-----	---

45	Quer utilizar <i>Smartphone</i>	0.03	0.900	0.009
46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	4.24	0.046	0.116*
48	Necessidade de tapar a câmara do <i>Smartphone</i>	0.00	1.000	0.002
49	Necessidade de desligar o GPS	0.05	0.905	0.013
50	Desligar o <i>Smartphone</i> no momento que não utiliza	1.12	0.278	0.061
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	0.23	0.635	0.027
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	0.11	0.812	0.019

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	0.79	0.395	0.050
59	Considera seguro de partilhar multimédia	0.63	0.960	0.044
60	Sente seguro para comunicar-se com contactos e empresa	7.14	0.128	0.150
61	Sente seguro para jogar em diversas aplicações	2.19	0.701	0.083

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 58 - Teste Qui-quadrado de Independência e V de Crámer por Geração dos estudantes

Grupo 4

Item	Cruzamento	χ^2	sig	V
19	Houve alturas que se preocupou com a privacidade	1.26	0.869	0.063
20	Não comprava um <i>Smartphone</i> se voltasse atrás	-	-	0.125
21	As funcionalidades não são consistentes como esperava	2.28	0.685	0.085
22	Sempre teve certeza de como era a utilização do <i>Smartphone</i>	11.16	0.025	0.188*
26	Conhecendo os riscos de segurança, para de usar <i>Smartphone</i>	-	-	0.085

Grupo 8

Item	Cruzamento	χ^2	sig	V
45	Quer utilizar <i>Smartphone</i>	4.78	0.310	0.123

46	Intenção de aumentar o uso das ferramentas do <i>Smartphone</i>	7.53	0.110	0.154
48	Necessidade de tapar a câmara do <i>Smartphone</i>	4.37	0.358	0.117
49	Necessidade de desligar o GPS	3.12	0.538	0.099
50	Desligar o <i>Smartphone</i> no momento que não utiliza	-	-	0.088
51	Adquirir aplicação para defender de invasão no <i>Smartphone</i>	2.32	0.678	0.085
52	Ter botão para ligar/desligar o microfone do <i>Smartphone</i>	5.40	0.248	0.131

Grupo 10

Item	Cruzamento	χ^2	sig	V
58	Divulga informações pessoais no <i>Smartphone</i>	4.24	0.374	0.116
59	Considera seguro de partilhar multimédia	-	-	0.169*
60	Sente seguro para comunicar-se com contactos e empresa	-	-	0.138**
61	Sente seguro para jogar em diversas aplicações	-	-	0.132

Nota: *Nível de significância de 5% ($\alpha = 0,05$), ** Nível de significância de 10% ($\alpha = 0,10$)

Tabela 59 - Teste Qui-quadrado de Independência e V de Crámer por Curso dos estudantes

Apêndice C – Conclusões por objetivo de investigação

Conclusões por objetivo de investigação

4.2.14. Conclusões por objetivo de investigação

De forma a responder às questões de investigação, realizou-se uma análise estatística aos itens do questionário, o que permitiu determinar se existe uma indicação de dependência e qual o grau de associação com as variáveis sexo, geração e curso. Os testes realizados, nesta análise, foram o teste qui-quadrado de independência, para verificar a influência, e a correlação de V de *Crámer*, de forma a avaliar o grau de associação/relação entre as variáveis selecionadas com uma maior importância estatística para o estudo (44) e as três variáveis socio demográficas sexo, geração e curso. As restantes variáveis (15) do questionário foram analisadas de forma descritiva. Os gráficos gerados permitiram obter a informação procurada, de maneira a responder aos objetivos do estudo. O último teste gerado foi o teste da razão de chance (*Odds Ratio*), que permite avaliar a possibilidade de um evento que acontece num grupo ocorrer num outro grupo. Este teste foi aplicado às variáveis com uma maior importância estatística, determinadas com o teste do Qui-Quadrado e V *Crámer*, anteriormente.

4.2.15. Determinar o nível de confiança desta população com as organizações;

A primeira questão de investigação deste estudo procurou determinar o nível de confiança dos estudantes com as organizações que tratam os seus dados registados pelo *Smartphone*. De forma a poder responder a esta questão, foi analisado um conjunto de 21 perguntas, criadas a partir do modelo *TUM*, utilizado neste estudo – primeiro, de forma descritiva e, de seguida, foi feita uma análise estatística, utilizando a ferramenta *SPSS*.

Ao analisar as variáveis do grupo da teoria do nível de adaptação (*c.f.* apêndice A), verificou-se que 32,2% dos estudantes considerava, previamente a ter um *Smartphone*, que este teria poucos riscos para a sua privacidade, havendo quem considerasse que teria bastantes riscos (30,2%). Constatou-se que 37,9% dos estudantes tinha pouca confiança na partilha de informação inerente à utilização das aplicações necessárias ao funcionamento do *Smartphone*. Uma conclusão interessante corresponde ao facto de 91,2% dos inquiridos afirmar que, relativamente aos dados que partilhariam pelo *Smartphone*, através dos dados móveis, já antes de ter um dispositivo, existem, no

mínimo, poucos riscos de privacidade. Assim, é possível encontrar alguma incerteza ou desconfiança por parte da maioria dos estudantes, na utilização do *Smartphone*. O estudo também mostra que 30% dos alunos considerava que a utilização da câmara do *Smartphone* oferecia poucos riscos de segurança e 33,8% não viu qualquer necessidade de instalar uma aplicação para manter o seu direito à privacidade, quando utiliza este aparelho, mostrando, assim, que alguns estudantes ponderam a existência de um risco de privacidade associado ao uso do *Smartphone*.

Na análise do grupo da dissonância cognitiva (*c.f.* apêndice A), notou-se que existem momentos em que a grande maioria dos estudantes (77,9%) se preocupa com a sua privacidade, ao utilizar o *Smartphone*. A maior parte (96,2%) voltaria a comprar um *Smartphone*, se pudesse voltar atrás. Quase metade dos estudantes (49,8%) teve inconsistências com algumas funcionalidades, ao usar este telemóvel, comparando com as expectativas que tinham antes do uso. A grande maioria confia no seu *Smartphone* (80,8%), sente-se confortável ao usá-lo (94,6%) e diz que o utilizou corretamente (90,5%). Verificou-se, neste grupo, que, de um modo geral, os estudantes confiam no seu *Smartphone*, apesar de terem alturas em que se preocupam com a sua privacidade.

Quanto ao grupo da intenção comportamental (*c.f.* apêndice A), verificou-se que a grande maioria dos estudantes (70,7%) não tem necessidade de tapar a câmara do *Smartphone* em algumas situações. No entanto, 58,4% tem a necessidade de desligar o GPS, no *Smartphone*, sempre que não necessita. Relativamente à necessidade de desligarem o *Smartphone* em períodos que não o estão a utilizar, por questões de segurança, a grande maioria (92,4%) não a sente. Também a generalidade dos académicos (59,3%) indicou não ter qualquer intenção de adquirir uma aplicação para se defender da invasão de terceiros. 58% adorava ter um botão que permitisse ligar e desligar o microfone. Estes resultados indicam que a maior parte dos estudantes não tenciona tomar medidas para proteger a sua privacidade, na utilização do *Smartphone*.

Em relação ao grupo da confiança e segurança do questionário (*c.f.* apêndice A), verificou-se que a grande maioria dos alunos (64%) divulga as suas informações pessoais no *Smartphone*. No que diz respeito à partilha de fotografias, vídeos, ficheiros e informações pessoais, 47,6% dos estudantes considera o *Smartphone* um meio seguro (segurança neutra) e 28,7% considera pouco seguro. No que toca à utilização do *Smartphone* para comunicar com os seus contactos ou empresas, 43,5% dos discentes

sente-se medianamente seguro (segurança neutra) e 33,8% considera bastante seguro. Quanto à questão que procura saber se os inquiridos se sentem seguros ao utilizar o *Smartphone* para jogar as mais diversas aplicações, 41,3% indicou que sente uma segurança neutra, existindo, também, 29,3% a indicar que se sente bastante seguro. Na questão que pretende saber se estes universitários se sentem seguros ao utilizar o *Smartphone* para ter conversas privadas relacionadas com trabalho ou dados sensíveis, 40,1% considera que se sente medianamente seguro (segurança neutra) e 24,3% respondeu que se sente bastante seguro. Com base na análise descritiva, é possível verificar que, apesar de os estudantes considerarem o *Smartphone* um meio de segurança neutra para a partilha de dados e para a comunicação, utilizam-no para esses efeitos e também divulgam as suas informações pessoais no mesmo.

Além do referido, verificou-se que os inquiridos não confiam e/ou têm certas incertezas relativamente a questões de confiança para com as organizações que lhes disponibilizam os serviços e ferramentas no *Smartphone*. Ainda assim, utilizam-nos frequentemente, incluindo informações pessoais no telemóvel.

Através da análise dos testes gerados no *SPSS* com a variável sexo (Tabela 4, *c.f.* apêndice B), verificou-se que existe uma indicação estatística de dependência e um grau de associação/correlação com os itens 15 (confia a partilha de informação), item 16 (utilização do mesmo tem risco aos dados móveis), item 18 (instalar um aplicação para manter a privacidade), item 19 (houve alturas que se preocupou com a privacidade), item 20 (não comprava um *Smartphone* se voltasse atrás), item 23 (confia no *Smartphone*), item 24 (sente-se confortável ao usar o *Smartphone*), item 48 (necessidade de tapar a câmara do *Smartphone*) e item 50 (desligar o *Smartphone* no momento que não utiliza), com nível de significância de 5% e 10%.

Após verificar as variáveis associadas ao sexo, procurou-se averiguar a razão de chances (*odds ratio*), como pode ser observado na Tabela 5 (*c.f.* apêndice B). Ressalta-se que as únicas variáveis testadas foram as que mostraram ter dependência (χ^2), ter associação (*V*) e serem de natureza dicotómica (possuírem duas categorias). As variáveis que apresentaram significância estatística correspondem aos itens 19, 23, 48 e 50. Através desta análise, verificou-se que, quanto a momentos de preocupação com a privacidade, ao utilizar o *Smartphone*, os rapazes têm metade das possibilidades de ter essas ocorrências, quando contrastados com as raparigas. São também eles que têm o dobro das

probabilidades (208%) de confiar no *Smartphone*, comparativamente com as raparigas. Ainda num contraste entre os dois sexos, o masculino tem 74% menos de hipóteses de sentir alguma necessidade de tapar a câmara, em certas circunstâncias, e tem uma chance três vezes e meia (357%) superior de sentir a necessidade de desligar o *Smartphone*, em momentos de inatividade com o aparelho.

Denotou-se a existência de uma indicação estatística de dependência e um grau de associação/correlação com os itens 15 (confia a partilha de informação), item 17 (utilização da câmara tem risco de segurança) e item 18 (instalar uma aplicação para manter a privacidade), com nível de significância de 5% e 10%, com a análise dos testes gerados da variável geração (Tabela 6, *c.f.* apêndice A). Verificou-se que existe uma diferença de opinião entre as gerações, relativamente à confiança na partilha de informação, ao risco de segurança na utilização da câmara e à instalação de uma aplicação para manter a privacidade.

A indicação estatística de associação/correlação com os itens 24 (sente-se confortável ao usar o *Smartphone*), item 59 (considera seguro de partilhar multimédia) e item 60 (sente seguro para comunicar-se com contactos e empresa), com nível de significância de 5% e 10%, foi notória com a análise resultante dos testes gerados com a variável curso (Tabela 7, *c.f.* apêndice B).

4.2.16. Determinar se a população em estudo se sente segura relativamente à sua privacidade pessoal ao usar o *Smartphone* e as suas aplicações;

Neste contexto, analisou-se um conjunto de 21 perguntas, criadas a partir do modelo *TUM*, utilizado neste estudo. Inicialmente, de forma descritiva e, de seguida, foi feita uma análise estatística, utilizando a ferramenta *SPSS*.

Com base na análise das variáveis do grupo da teoria do nível de adaptação (*c.f.* apêndice A), constatou-se que, previamente à aquisição de um *Smartphone*, 32,2% dos estudantes considerava a existência de poucos riscos para a sua privacidade, contrariamente a 30,3% que associa o uso deste equipamento a um risco elevado no que diz respeito à privacidade. 37,9% tem pouca confiança na partilha de informação inerente à utilização das aplicações necessárias ao funcionamento do *Smartphone*. Denotou-se alguma incerteza e desconfiança por parte da maioria dos inquiridos, na utilização deste aparelho, uma vez que 91,2% afirmou que existem riscos de privacidade (ainda que

possam ser poucos), relativamente aos dados que iriam partilhar, via dados móveis. O estudo mostrou também que 30% considera a existência de poucos riscos de segurança com a utilização da câmara do *Smartphone* e 33,8% não viu necessidade de manter o seu direito à privacidade com a instalação de uma aplicação para esse fim.

Apesar de a grande maioria dos estudantes confiar no seu *Smartphone* (80,8%), sentir-se confortável ao usá-lo (94,6%) e afirmar que o utilizou corretamente (90,5%), a elevada percentagem de 77,9% teve momentos durante os quais se preocupou com a sua privacidade ao utilizar este dispositivo, analisando o grupo da dissonância cognitiva (*c.f.* apêndice A). Os universitários, de um modo geral, preocupam-se com a sua privacidade relativamente ao uso do *Smartphone*, mas, ao mesmo tempo, confiam nele e sentem-se confortáveis ao utilizá-lo.

No que remete para o grupo da intenção comportamental (*c.f.* apêndice A), verificou-se que 53,3% dos alunos tenciona aumentar o uso das ferramentas do *Smartphone* e 81,1% queria ter novas ferramentas no seu telemóvel. Apesar de 58,4% ter a necessidade de desligar o GPS no *Smartphone* sempre que não o necessita, 70,7% demonstrou não ter preocupação em tapar a câmara em algumas situações. Em períodos de inatividade, 92,4% afirmou não ver necessidade em desligar o *Smartphone*, por questões de segurança. A possibilidade de instalar uma aplicação para proteger a invasão de terceiros não suscitou interesse a 59,3% dos alunos, mas 58% gostaria de ter um botão que permitisse ligar e desligar o microfone. Assim, constatou-se que a maior parte dos estudantes tenciona aumentar o número e o uso das ferramentas no *Smartphone*, mas não pretende tomar medidas para proteger a sua privacidade com essa utilização.

Quanto ao grupo da confiança e segurança do questionário (*c.f.* apêndice A), constatou-se que a maioria dos universitários (64%) divulga as suas informações pessoais no *Smartphone*. 47,6% dos inquiridos considera este telemóvel medianamente seguro (segurança neutra) e 28,7% vê-o como algo pouco seguro, no que diz respeito à partilha de fotografias, vídeos, ficheiros e informações pessoais. Para comunicar com contactos ou empresas, 43,5% sente-se medianamente seguro (segurança neutra) com a utilização deste aparelho, havendo 33,8% que o encaram como algo bastante seguro. O uso de *Smartphones* para jogar as mais diversas aplicações deixa 41,3% medianamente seguro (segurança neutra) e 29,3% afirma que se sente muito seguro. No que toca a conversas privadas relacionadas com trabalho ou outros dados sensíveis, 40,1% considera o

telemóvel medianamente seguro (segurança neutra) e 24,3% denota uma elevada segurança.

Com base na análise descritiva, é possível verificar que, apesar de os estudantes considerarem o *Smartphone* um meio de segurança neutra para a partilha de dados e para a comunicação, utilizam-no para esses efeitos e também divulgam as suas informações pessoais no mesmo. Note-se que existe a indicação de que os estudantes não se sentem seguros, relativamente à sua privacidade, ao utilizar o *Smartphone*.

Na análise dos dados com o *SPSS* (*c.f.* apêndice B), verificou-se o referido acima – a inexistência de segurança relativamente à privacidade com o uso do *Smartphone*. Para ilustrar esta observação, foi realizado o teste qui-quadrado de independência, verificando a influência e a correlação de *V* de *Crámer*, para avaliar o grau de associação/relação entre algumas variáveis dos grupos 3, 4, 8 e 10 do questionário com as variáveis sexo, geração e curso.

A análise aos testes gerados com a variável sexo (Tabela 8, *c.f.* apêndice B) permitiu denotar a existência de uma indicação estatística de independência e de um grau de associação/correlação com o item 15 (confia a partilha de informação), item 16 (utilização do mesmo tem risco aos dados móveis), item 18 (instalar um aplicação para manter a privacidade), item 19 (houve alturas que se preocupou com a privacidade), item 23 (confia no *Smartphone*), item 24 (sente-se confortável ao usar o *Smartphone*), item 46 (intenção de aumentar o uso das ferramentas do *Smartphone*), item 47 (adorava ter novas ferramentas no *Smartphone*), item 48 (necessidade de tapar a câmara do *Smartphone*) e item 50 (desligar o *Smartphone* no momento que não utiliza), com nível de significância de 5% e 10%.

Posteriormente à verificação das variáveis associadas ao sexo, procurou-se averiguar a razão de chances (*odds ratio*), como se pode observar na Tabela 9 (*c.f.* apêndice B). As que mostraram ter dependência (χ^2), ter associação (*V*) e serem de natureza dicotómica (possuírem duas categorias) foram as únicas variáveis testadas. As que apresentaram significância estatística correspondem aos itens 19, 23, 46, 47, 48 e 50. Observou-se que os rapazes, comparativamente com as raparigas, apresentam metade das chances de ter tido momentos durante os quais se preocuparam com a sua privacidade, ao usar o *Smartphone*. No que diz respeito à confiança no uso deste telemóvel, o sexo masculino

tem uma possibilidade superior (208%) à do sexo feminino. São também os rapazes que têm mais de duas vezes e meia (263%) de chances de aumentar o uso das ferramentas deste aparelho, assim como de adorar a ideia de ter novas ferramentas no mesmo (257%). São eles que têm quase menos três terços (26%) de possibilidades de sentir alguma necessidade de tapar a câmara em determinadas situações, assim como têm mais de três vezes e meia (357%) de probabilidades de desligar o telemóvel quando não o necessitam, em relação às raparigas.

A existência de uma indicação estatística de dependência e de um grau de associação/correlação com os itens 15 (confia a partilha de informação), item 17 (utilização da câmara tem risco de segurança), item 18 (instalar uma aplicação para manter a privacidade) e item 46 (intenção de aumentar o uso das ferramentas do *Smartphone*), com nível de significância de 5% e 10%, verificou-se com a análise dos testes gerados da variável geração (Tabela 10, *c.f.* apêndice B). Relativamente à confiança na partilha de informação, ao risco de segurança na utilização da câmara, à instalação de uma aplicação para manter a privacidade e à intenção de aumentar o uso das ferramentas do *Smartphone*, observou-se uma diferença de opinião entre as gerações.

Com o balanço resultante dos testes gerados com a variável curso (Tabela 11, *c.f.* apêndice A), verificou-se uma indicação de grau de associação/correlação com os itens 24 (sente-se confortável ao usar o *Smartphone*), item 59 (considera seguro de partilhar multimédia) e item 60 (sente seguro para comunicar-se com contactos e empresa), com nível de significância de 5% e 10%.

Mostrou-se que existe uma diferença de opinião entre os cursos, relativamente ao facto de se sentir confortável ao usar o *Smartphone* para efeitos de partilha de multimédia, assim como para comunicar com contactos e com a empresa.

4.2.17. Determinar o nível de satisfação do tratamento dos dados privados da população pelas organizações;

Como resposta a este ponto, analisou-se – primeiro, de forma descritiva e, de seguida, através de uma análise estatística, utilizando a ferramenta *SPSS* - um conjunto de 14 perguntas, criadas a partir do modelo *TUM*, utilizado neste estudo.

Ao analisar as variáveis do grupo da teoria do nível de adaptação (*c.f.* apêndice A), verificou-se que 37,9% dos estudantes considerava que confiaria pouco na partilha de informação inerente à utilização das aplicações necessárias ao funcionamento do *Smartphone* e 36,9% considerava que teria uma confiança mediana (confiança neutra). Observou-se que 36,9% dos inquiridos considerava, previamente a ter um *Smartphone*, que a utilização teria alguns riscos de privacidade relativamente aos dados móveis que partilhariam. O estudo também mostra que os alunos consideravam que a utilização da câmara do *Smartphone* ofereceria poucos riscos de segurança (30%) e que não seria necessário instalar uma aplicação para manter o seu direito à privacidade, previamente a ter um desses telemóveis (33,8%). Tal mostra que os estudantes estão cientes de que existe um risco de privacidade associado ao uso do *Smartphone*.

No que diz respeito ao grupo da intenção comportamental (*c.f.* apêndice A), verificou-se que a grande maioria dos estudantes não tem a necessidade de tapar a câmara (70,7%) em algumas situações. No entanto, uma grande percentagem de 58,4% tem a necessidade de desligar o *GPS* no *Smartphone*, sempre que não precisa dele. Relativamente à necessidade de desligarem o *Smartphone* em períodos que não o estão a utilizar, por questões de segurança, a grande maioria (92,4%) não a sente. A maior parte dos discentes (59,3%) também indicou não ter a intenção de adquirir uma aplicação para se defender da invasão de terceiros, havendo 58% que gostaria de ter um botão que permitisse ligar e desligar o microfone. Estes resultados indicam que a maior parte dos estudantes não se importa com o risco de a câmara do *Smartphone* estar exposta, tendo-se constatado que não tencionam tomar medidas para proteger a sua privacidade durante o uso do telemóvel.

Quanto ao grupo da confiança e segurança do questionário (*c.f.* apêndice A), denotou-se que a grande maioria dos estudantes (64%) divulga as suas informações pessoais no *Smartphone*. 47,6% dos estudantes considera o *Smartphone* medianamente seguro (segurança neutra) e 28,7% considera pouco seguro, relativamente à partilha de fotografias, vídeos, ficheiros e informações pessoais. No que toca ao uso do *Smartphone* para comunicar com os seus contactos ou empresas, 43,5% dos estudantes sente-se medianamente seguro (segurança neutra) e 33,8% refere que se sente bastante seguro. Em relação à questão que procura averiguar se os estudantes se sentem seguros ao utilizar o *Smartphone* para jogar as mais diversas aplicações, 41,3% dos inquiridos indicou que se sente medianamente seguro (segurança neutra) e 29,3% indicou que se sente bastante seguro. Na questão que tinha o propósito de saber se os estudantes se sentem seguros, ao

utilizar o *Smartphone*, para ter conversas privadas relacionadas com trabalho ou dados sensíveis, 40,1% considera que se sente medianamente seguro (segurança neutra) e 24,3% que se sente bastante seguro.

Com base na análise descritiva, é possível constatar que a maior parte dos universitários não apresenta grandes preocupações com o tratamento dos dados privados, recolhidos pelo *Smartphone*, aos quais as organizações podem aceder. Note-se, no entanto, que há uma percentagem relativamente considerável que parece preocupar-se com esta questão.

Na análise com o *SPSS* (c.f. apêndice B), verificou-se que existe a indicação de que a insatisfação dos estudantes, perante o tratamento de dados privados recolhidos pelas organizações, não é muito elevada. Para caracterizar esta observação, foi realizado o teste qui-quadrado de independência, de forma a verificar a influência e a correlação de *V* de *Crámer*, com o propósito de avaliar o grau de associação/relação entre algumas variáveis dos grupos 3, 8 e 10 do questionário, com as variáveis sexo, geração e curso.

Graças à análise dos testes gerados com a variável sexo (Tabela 12, c.f. apêndice B), comprovou-se uma indicação estatística de independência e um grau de associação/correlação com os itens 15 (confia a partilha de informação), item 16 (utilização do mesmo tem risco aos dados móveis), item 18 (instalar uma aplicação para manter a privacidade), item 48 (necessidade de tapar a câmara do *Smartphone*) e item 50 (desligar o *Smartphone* no momento que não utiliza), com nível de significância de 5% e 10%. Conclui-se que, nestes itens, existe uma diferença de opiniões significativa entre os sexos.

Tal como pode ser observado na Tabela 13 (c.f. apêndice B), procurou-se averiguar a razão de chances (*odds ratio*). Atente-se para o facto de que as únicas variáveis testadas foram as que mostraram ter dependência (χ^2), ter associação (*V*) e serem de natureza dicotómica (possuírem duas categorias). Os itens 48 (Necessidade de tapar a câmara do *Smartphone*) e 50 (Desligar o *Smartphone* no momento que não utiliza) correspondem às que apresentaram significância estatística. Destaca-se que os rapazes têm quase menos de três quartos (0,26%) de necessidade de tapar a câmara do *Smartphone*, em certas situações, do que as raparigas. Também os rapazes sentem mais de três vezes e meia

(357%), comparativamente com as raparigas, a necessidade de desligar este telemóvel por completo, durante os períodos em que não o usam.

Denotou-se, em consequência da análise dos testes gerados da variável geração (Tabela 14, *c.f.* apêndice B), que existe uma indicação estatística de dependência e um grau de associação/correlação com os itens 15 (confia a partilha de informação), item 17 (utilização da câmara tem risco de segurança) e item 18 (instalar uma aplicação para manter a privacidade), com nível de significância de 5% e 10%. Assim sendo, foi possível concluir que existe uma diferença de pontos de vista entre as gerações, relativamente ao facto de confiar a partilha de informação no *Smartphone*, de haver riscos de segurança com a utilização da câmara do mesmo e de surgir a necessidade de instalar uma aplicação para manter a privacidade no telemóvel.

A avaliação dos testes gerados com a variável curso (Tabela 15, *c.f.* apêndice B) levou-nos a verificar a existência de uma indicação estatística de dependência e de um grau de associação/correlação com os itens 59 (considera seguro de partilhar multimédia) e item 60 (sente-se seguro para comunicar-se com contactos e com a empresa), com nível de significância de 5% e 10%. Deste modo, denotaram-se diferentes posições entre os cursos, no que diz respeito aos aspetos referidos.

4.2.18. Determinar o comportamento com o *Smartphone* ligado à internet, GPS, câmara, microfone;

Não só de uma forma descritiva, mas também através de uma análise estatística na qual se utilizou a ferramenta *SPSS*, analisou-se, no contexto desta questão, um conjunto de 13 perguntas, criadas a partir do modelo *TUM*, utilizado neste estudo.

Ao analisar as variáveis do grupo do perfil tecnológico, verificou-se que mais de metade dos estudantes utiliza o *Smartphone* ligado à internet para participar nas redes sociais, ver vídeos, pesquisar conteúdos, navegar nas páginas da internet e/ou consultar o e-mail. A maioria dos alunos liga-se à internet com o *Smartphone*, a partir da sua rede *Wi-Fi* privada de casa, da rede móvel privada da sua operadora de telecomunicações e de redes *Wi-Fi* em lugares públicos. Observou-se que todas as aplicações do *Smartphone* avaliadas neste estudo são usadas, pelo menos, por metade dos inquiridos e que a maioria está online na sua aplicação favorita, várias vezes por dia.

No que respeita ao grupo da intenção comportamental (*c.f.* apêndice A), verificou-se que a grande maioria dos estudantes (81,1%), no futuro, adorava ter novas ferramentas no seu *Smartphone*. A necessidade de tapar a câmara do *Smartphone*, em algumas situações, é inexistente para 70,7%, mas no que diz respeito à necessidade de desligar o GPS sempre que não é necessário, 58,4% manifesta-a. A grande maioria dos universitários (92,4%) não sente a necessidade de desligar o *Smartphone* por completo durante os períodos em que não o está a utilizar, por questões de segurança. 59,3% não tem a intenção de adquirir uma aplicação para se defender da invasão de terceiros e 58% gostaria de ter um botão que permitisse ligar e desligar o microfone do seu *Smartphone*. Estes resultados indicam que a maior parte dos estudantes não se importa com o risco de a câmara do *Smartphone* estar exposta nas várias situações, tendo-se verificado que, apesar disso, não tenciona tomar medidas para proteger a sua privacidade. A análise exploratória dos dados da intenção comportamento mostrou que os estudantes adorariam ter ferramentas novas no seu telemóvel, ou seja, tencionam utilizar mais ferramentas neste tipo de dispositivos, no futuro. Não sentem a necessidade de tapar a câmara, não têm a intenção de instalar uma aplicação no *Smartphone* para proteger a sua privacidade, mas a maioria dos alunos adorava ter um botão que permitisse ligar e desligar o microfone do mesmo.

Na apreciação das variáveis do grupo sobre o uso real (UR) (*c.f.* apêndice A), apurou-se que, de todas as funcionalidades apresentadas (Páginas *WEB*, GPS, Calendário, e-mail, contactos, câmaras, microfone, mensagens) aos inquiridos, apenas o microfone não é utilizado por, pelo menos, metade dos estudantes. 86,4% utiliza o *Smartphone* todos dias e 63,4% não utiliza o GPS neste aparelho, para atividades físicas.

O comportamento dos estudantes com o *Smartphone* ligado à internet (*c.f.* apêndice A), segundo os dados analisados, é bastante intensivo, havendo uma utilização diária do telemóvel, assim como das várias aplicações e ferramentas do mesmo, conectadas à internet. Constatou-se que os estudantes se conectam a esta, através de redes privadas e públicas, o que denota um maior risco de invasão de privacidade. Com as funcionalidades do *Smartphone*, que são capazes de registar dados mais críticos para a privacidade de cada indivíduo como a câmara, o *GPS* e o microfone, verificou-se que os estudantes utilizam estas ferramentas e não parecem ter um cuidado especial para se protegerem dos potenciais riscos envolvidos.

Com o auxílio dos testes gerados na ferramenta *SPSS* com a variável sexo (*c.f.* apêndice B), observou-se (Tabela 16) uma indicação estatística de dependência e um grau de associação/correlação com o item 47 (adorava ter novas ferramentas no *Smartphone*), item 48 (necessidade de tapar a câmara do *Smartphone*), item 50 (desligar o *Smartphone* no momento que não utiliza) e item 57 (Usa GPS para atividades físicas e desportivas), com nível de significância de 5% e 10%.

Depois de verificar as variáveis associadas ao sexo, averiguou-se a razão de chances (*odds ratio*), como se observa na Tabela 17 (*c.f.* apêndice B). Tal como referido em contextos anteriores, note-se que apenas se testaram variáveis que mostrassem ter dependência (χ^2), ter associação (*V*) e serem de natureza dicotómica (possuírem duas categorias). As que apresentaram significância estatística correspondem aos itens 47, item 48, item 50 e item 57. Neste contexto, as possibilidades de os rapazes apresentam-se mais de duas vezes e meia superiores (257%) às das raparigas, no que diz respeito à eventualidade de gostarem de ter novas ferramentas no *Smartphone*. O sexo masculino reflete uma necessidade inferior em quase três quartos (0,26%) quanto à necessidade de tapar a câmara do *Smartphone* e denota uma necessidade três vezes e meia superior (357%) de desligar o telemóvel por completo durante os períodos em que não o usa, comparativamente com o sexo feminino. Para atividades físicas/desportivas, a utilização do GPS do *Smartphone* é mais provável por parte dos rapazes – 83%.

Com nível de significância de 10%, verificou-se a existência estatística de dependência e um grau de associação/correlação com o item 57 (Usa *GPS* para atividades físicas e desportivas), através dos testes gerados com a variável geração (Tabela 18, *c.f.* apêndice B).

Dentro dos testes gerados com a variável curso (Tabela 19, *c.f.* apêndice B), não se validou a existência de uma indicação estatística de dependência e um grau de associação/correlação, com nível de significância de 5% e 10%. Pode-se concluir que não existe uma diferença significativa, nesta questão de investigação, entre os cursos.

4.2.19. Determinar se a população estudada sabe que tipo de informações está a disponibilizar aos vários tipos de organizações;

A partir do modelo *TUM*, utilizado no estudo desta dissertação, criou-se um conjunto de 18 perguntas, que foram analisadas de forma descritiva e através de uma análise estatística, utilizando a ferramenta *SPSS*, com o intuito de dar uma resposta a esta questão.

Denotou-se que a maioria dos estudantes inclui, no perfil da conta do seu *Smartphone*, o nome real (86,4%), endereço de e-mail (76,3%), número de telefone (63,1%) e fotografias pessoais (62,1%), ao estudar as variáveis do grupo do perfil tecnológico (*c.f.* apêndice A). 74,1% sabe que terceiros utilizam os seus dados pessoais registados pelo *Smartphone* e 74,8% aceita os termos de aceitação, quando estes implicam ter acesso aos dados de posicionamento do seu telemóvel. Observou-se, então, que os alunos introduzem no *Smartphone* dados que facilitam a identificação do utilizador, mesmo indicando que têm conhecimento da possibilidade de terceiros utilizarem os seus dados privados registados e aceitam os termos de aceitação, quando implicam o alcance a dados de posicionamento.

Concluída a análise das variáveis do grupo da teoria do nível de adaptação (*c.f.* apêndice A), verificou-se que 37,9% dos estudantes considerava confiar pouco na partilha de informação inerente à utilização das aplicações necessárias ao funcionamento do *Smartphone* e 36,9% confiava medianamente (confiança neutra). 36,9% dos estudantes considerava, previamente a ter um *Smartphone*, que a utilização teria alguns riscos de privacidade relativamente aos dados móveis que partilharia. O estudo também mostra que os alunos encaram a utilização da câmara do *Smartphone* pouco arriscada quanto a questões de segurança (30%) e não reconhecem a necessidade de instalar uma aplicação para manter o seu direito à privacidade (33,8%), mostrando, assim, que estão cientes de que existe um risco de privacidade associado ao uso do *Smartphone*.

Na análise das variáveis do grupo da teoria da dissonância cognitiva (*c.f.* apêndice A), verificou-se que os estudantes, na sua grande maioria (77,9%), já tiveram momentos nos quais se preocuparam com a sua privacidade, ao utilizar o *Smartphone*, mas, ao mesmo tempo, quase todos eles (96,5%) responderam que não vão deixar de o utilizar, ainda que tenham conhecimento dos riscos de segurança associados.

No grupo da utilidade percebida, verificou-se que a maior parte dos discentes (52,1%) considera útil a possibilidade de partilhar fotografias, vídeos e ficheiros pelo *Smartphone*.

No que toca à análise do grupo sobre o uso real (UR), observou-se que a maioria dos alunos (93,7%) utiliza o *Smartphone* para partilhar dados e fotografias. Para a monitorização da atividade física/desportiva, a maior parte (56,8%) não utiliza o *Smartphone* e 63,4% também não costuma utilizar o *GPS* do mesmo, nas suas atividades físicas.

No que diz respeito ao grupo da confiança e segurança do questionário (*c.f.* apêndice A), 64% dos estudantes divulga as suas informações pessoais no *Smartphone*. Relativamente à partilha de fotografias, vídeos, ficheiros e informações pessoais, 47,6% encara o *Smartphone* medianamente seguro (segurança neutra) e 28,7% vê-o como um aparelho pouco seguro (28,7%). No que respeita à utilização do *Smartphone* para comunicar com os seus contactos ou empresas, 43,5% sente-se medianamente seguro (segurança neutra) e 33,8% sente-se bastante seguro. Em relação à questão que procura saber se os estudantes se sentem seguros ao utilizar este telemóvel para jogar as mais diversas aplicações, 41,3% indicou que sente uma segurança intermédia (segurança neutra) e 29,3% afirmou que se sente bastante seguro. Na questão que pretende averiguar se os inquiridos se sentem seguros ao utilizar o *Smartphone* para ter conversas privadas relacionadas com trabalho ou dados sensíveis, 40,1% sente-se medianamente seguro (segurança neutra) e 24,3% respondeu que se sente bastante seguro.

A população em estudo mostrou indicadores sobre a incerteza do conhecimento do tipo de informações que está a disponibilizar às várias organizações, o que também pode explicar as dúvidas observadas, nas quais se verificou que não sabem se devem ou não confiar nas organizações e que já tiveram momentos de preocupação relativamente à sua privacidade. Visto que os estudantes disponibilizam informações pessoais no *Smartphone* e têm inseguranças relacionadas com a sua privacidade, constatou-se que sabem, pelo menos, que existe a possibilidade de as organizações utilizarem mais dados sobre eles do que aqueles de que têm conhecimento.

Partindo dos testes gerados no *SPSS* com a variável sexo, denotou-se (Tabela 20, *c.f.* apêndice B) uma indicação estatística de dependência e um grau de associação/correlação com os itens 12 (aceita termos de aceitação), item 15 (confia a partilha de informação),

item 16 (utilização do mesmo tem risco aos dados móveis), item 18 (instalar um aplicação para manter a privacidade), item 19 (houve alturas que se preocupou com a privacidade ao usar *Smartphone*), item 55 (costuma usar *Smartphone* para partilhar multimídia) item 57 (usa *GPS* para atividades físicas e desportivas), com nível de significância de 5% e 10%.

Uma vez verificadas as variáveis associadas ao sexo, averiguou-se a razão de chances (*odds ratio*), como pode ser observado na Tabela 21 (*c.f.* apêndice A). Ressalta-se, uma vez mais, que as únicas variáveis testadas foram as que mostraram ter dependência (χ^2), ter associação (*V*) e serem de natureza dicotómica (possuírem duas categorias). Os itens 12, 19, 55 e 57 correspondem às que apresentaram alguma relevância estatística. Quanto ao consentimento dos termos de aceitação, quando implicam acesso aos dados de posicionamento do *Smartphone*, os rapazes apresentaram uma possibilidade duas vezes maior (212%) de o fazer, comparativamente com as raparigas. Também eles apresentaram uma probabilidade superior (183%) no que diz respeito à utilização do *GPS* do telemóvel para atividades físicas. No entanto, o sexo masculino demonstrou ter chances inferiores ao feminino, relativamente à sua preocupação com a privacidade ao utilizar este dispositivo – duas vezes inferior (50%) – e quanto ao uso do mesmo para partilhar dados/fotografias – inferior a três quartos (22%).

Constatou-se uma indicação da existência estatística de dependência e um grau de associação/correlação com os itens 11 (terceiros utilizam os dados), item 15 (confia a partilha de informação), item 17 (utilização da câmara tem risco de segurança), item 18 (instalar um aplicação para manter a privacidade), item 26 (conhecendo os riscos de segurança, para de usar *Smartphone*) e item 57 (usa *GPS* para atividades físicas e desportivas) com nível de significância de 5% e 10%, graças aos testes gerados com a variável geração (Tabela 22, *c.f.* apêndice B).

Após o estudo dos testes gerados com a variável curso (Tabela 23, *c.f.* apêndice B), denotou-se uma indicação estatística de grau de associação/correlação com o item 59 (considera seguro de partilhar multimídia) e item 60 (sente seguro para comunicar-se com contactos e empresa), sendo o nível de significância de 5% e 10%.

4.2.20. Determinar se a população em estudo aceita que as organizações tenham acesso a todos os dados privados introduzidos no *Smartphone*;

Utilizando a ferramenta *SPSS*, examinou-se um conjunto de 22 perguntas, criadas a partir do modelo *TUM*, utilizado neste estudo, de forma descritiva e também através de uma análise estatística.

Tal como referido anteriormente, a maioria dos estudantes, mesmo estando cientes de tal facto, concede o acesso dos seus dados privados a terceiros (74,1%) e autoriza os termos de aceitação, quando estes implicam o acesso aos dados de posicionamento (74,8%). Deste modo, as organizações têm permissão para aceder a todos os dados introduzidos no *Smartphone*, sendo os mais comuns o nome real (86,4%), endereço de e-mail (76,3%), número de telefone (63,1%) e fotografias pessoais (62,1%), com base na análise das variáveis do grupo do perfil tecnológico (*c.f.* apêndice A).

Tendo em conta a análise efetuada às variáveis do grupo da teoria do nível de adaptação (*c.f.* apêndice A), previamente a ter um *Smartphone*, 32,3% dos estudantes considera o uso das aplicações de comunicação do mesmo pouco arriscado no que toca à sua privacidade, havendo 30,3% que encara como bastante arriscado. Quanto à utilização da câmara do telemóvel, 30% acredita que oferece poucos riscos de segurança e quanto à necessidade de instalar uma aplicação que assegure direitos de privacidade, 33,8% não a valoriza. Os estudantes sabem que as organizações têm acesso aos seus dados, mas continuam a utilizar o *Smartphone*, o que demonstra que aceitam que estas tenham acesso aos dados introduzidos.

Na análise das variáveis do grupo da teoria da dissonância cognitiva (*c.f.* apêndice A), verificou-se que os discentes, na sua grande maioria (77,9%), já tiveram momentos de preocupação com a sua privacidade, ao utilizar o *Smartphone*. 62,5% dos estudantes indica que sempre teve a certeza de como era a utilização do *Smartphone* e 80,8% também indicou que confiou no seu *Smartphone*. Com 94,6% dos inquiridos a indicar que se sentiu confortável ao utilizá-lo, verificou-se que têm um certo nível de satisfação com o tratamento de dados feito pelas organizações que registam os dados deste telemóvel. A maior parte dos alunos (96,5%) respondeu que não vai deixar de utilizar o *Smartphone*, mesmo conhecendo os riscos de segurança associados a este equipamento. Apesar de, tal como referido, a maioria ter tido momentos de preocupação com a sua privacidade,

verificou-se que confiaram no seu telemóvel, ainda que registe inúmeros dados privados tratados pelas organizações, o que denota um certo nível de confiança relativamente às mesmas. Tal é igualmente confirmado com o facto de os alunos se sentirem confortáveis ao utilizar o *Smartphone* e de dizerem que não vão deixar de o utilizar.

Relativamente ao grupo da intenção comportamental (*c.f.* apêndice A), constatou-se que a maioria dos estudantes (70,7%) não parece preocupar-se com os dados registados pela câmara do *Smartphone*, visto que não sente necessidade de a tapar. Em períodos de inatividade, também não sente a necessidade de desligar o aparelho (92,4%), de forma a limitar os dados registados pelo mesmo, assim como não pretende adquirir alguma aplicação para proteger a sua privacidade de terceiros (59,3%). No entanto, verificou-se que 58,4% tem a necessidade de desligar o *GPS*, sempre que não o utiliza, e que 58% gostaria de ter um botão que permitisse ligar e desligar o microfone do seu *Smartphone*, o que limitaria o acesso a este tipo de registo de dados.

No que toca à análise do grupo sobre o uso real (UR) (*c.f.* apêndice A), verificou-se que a maior parte dos universitários utiliza quase todas as funcionalidades apresentadas (páginas web, *GPS*, calendário, e-mail, contactos, câmaras, microfone e mensagens), sendo a aplicação do microfone a única a obter uma percentagem de utilização inferior a 50%. Este aspeto comprova que estes estudantes permitem o registo de muitos dados privados pelo *Smartphone*.

Denotou-se, no que diz remete para o grupo da confiança e segurança no questionário (*c.f.* apêndice A), que 64% dos alunos divulga informações pessoais no *Smartphone*. Este telemóvel é considerado medianamente seguro (segurança neutra) por 47,6% dos inquiridos no que diz respeito à partilha de fotografias, vídeos, ficheiros e informações pessoais, por 43,5% no que toca à sua utilização para comunicar com contactos ou com a empresa, por 41,3% quando a finalidade é jogar as mais diversas aplicações e por 40,1% para conversas privadas relacionadas com trabalho ou dados sensíveis. No entanto, 28,7% considera-o pouco seguro para a partilha de fotografias, vídeos, ficheiros e informações pessoais. Relativamente aos outros três aspetos, houve alunos que manifestaram bastante segurança, sendo as percentagens, respetivamente, de 33,8%, de 29,3% e de 24,3%.

A população em estudo mostrou que divulga as informações de dados pessoais e privados no seu *Smartphone*, que aceita os termos de utilização e que tem conhecimento

de que terceiros possam acessar a estes dados. Apesar de terem conhecimento dos riscos de privacidade envolvidos e de já terem tido momentos de preocupação com esses riscos, mantêm a confiança no seu *Smartphone* e não tencionam deixar de o utilizar. Não se verificaram comportamentos específicos de proteção por parte dos estudantes, o que reflete que, pelo menos até certo ponto, aceitam que as organizações que tratam todos estes dados tenham acesso aos mesmos.

Observou-se um grau de associação/correlação e uma indicação estatística de dependência com os itens 12 (aceita termos de aceitação), item 18 (instalar uma aplicação para manter a privacidade), item 19 (houve alturas que se preocupou com a privacidade), item 22 (sempre teve certeza de como era a utilização do *Smartphone*), item 23 (confia no *Smartphone*), item 24 (sente-se confortável ao usar o *Smartphone*), item 48 (necessidade de tapar a câmara do *Smartphone*) e item 50 (desligar o *Smartphone* no momento em que não utiliza), com nível de significância de 5% e 10%, a partir dos testes gerados com a variável sexo no SPSS (Tabela 24, *c.f.* apêndice B).

Apuradas as variáveis associadas ao sexo, explorou-se a razão de chances (*odds ratio*). As variáveis que apresentaram peso estatístico (Tabela 25, *c.f.* apêndice B) correspondem aos itens 12, 19, 22, 23, 48 e 50, tendo em conta que apenas se testaram as que mostraram ter dependência (χ^2), ter associação (*V*) e serem de natureza dicotómica (possuírem duas categorias). O consentimento dos termos de aceitação, quando implicam um acesso aos dados de posicionamento do *Smartphone*, é duas vezes maior nos rapazes (212%), assim como na confiança no equipamento (209%), comparativamente com as raparigas. Também os rapazes mostram chances superiores no que diz respeito a certezas da funcionalidade do telemóvel (70%) e ao facto de desligar este aparelho quando não o necessitam (357%). Por outro lado, o sexo masculino apresentou probabilidades duas vezes inferiores (50%) no que toca a preocupações de privacidade, ao utilizar o *Smartphone*, e uma chance inferior a três quartos (26%) relativamente à necessidade de tapar a câmara do mesmo, quando contrastado com o sexo feminino.

Atendendo aos testes gerados com a variável geração, verificou-se (Tabela 26, *c.f.* apêndice B) a existência estatística de dependência e um grau de associação/correlação com os itens 11 (terceiros utilizam os dados), item 17 (utilização da câmara tem risco de segurança), item 18 (instalar um aplicação para manter a privacidade) e item 26

(conhecendo os riscos de segurança, para de usar *Smartphone*), com nível de significância de 5% e 10%.

Constatou-se que existe um grau de associação/correlação com os itens 22 (Sempre teve certeza de como era a utilização do *Smartphone*), 59 (Considera seguro de compartilhar multimídia) e 60 (Sente-se seguro para comunicar com contactos e empresa), com nível de significância de 5% e 10%, mediante a pesquisa dos testes gerados com a variável curso (Tabela 27, *c.f.* apêndice B).

4.2.21. Determinar se o *Smartphone* traz vantagens no dia-a-dia para o utilizador;

Com o intuito de dar uma resposta a esta questão, criou-se, a partir do modelo *TUM*, utilizado neste estudo, um conjunto de 21 perguntas, que foram analisadas de forma descritiva. Posteriormente, fez-se uma análise estatística, com a ferramenta *SPSS*.

Com a análise das variáveis do grupo do perfil tecnológico (*c.f.* apêndice A), verificou-se que mais de metade dos estudantes utiliza o *Smartphone* ligado à internet para participar nas redes sociais, ver vídeos, pesquisar conteúdos, navegar nas páginas da internet e/ou consultar o e-mail. 41% dos estudantes sente que o *Smartphone* afeta os seus estudos de forma ligeiramente negativa e 25,9% sente que afeta de maneira ligeiramente positiva.

Quanto à apreciação das variáveis do grupo da teoria da dissonância cognitiva (*c.f.* apêndice A), observou-se que 49,8% dos estudantes teve um nível de dissonância, perante as expectativas de algumas funcionalidades, com a realidade, depois da sua utilização. 62,5% indicou que sempre teve a certeza de como era a utilização do *Smartphone*.

No grupo sobre a análise do uso do *Smartphone* (*c.f.* apêndice A), verificou-se que a maioria dos estudantes (95,6%) o utiliza para fins académicos.

Na avaliação sobre a facilidade de uso percebida (FUP) (*c.f.* apêndice A), verificou-se que os discentes (72,6%) consideram muito fácil comunicar com os seus contactos, através do *Smartphone*. As suas ferramentas são vistas pela maioria (93,7%) como flexíveis, de forma a poder usá-las como melhor lhe convier. 60,9% considera a partilha de fotos, vídeos e estados, no *Smartphone*, muito fácil. Quanto à interação com este aparelho, 44,2% julga-a bastante flexível e 43,2% encara-a como muito flexível.

No grupo da utilidade percebida do questionário (*c.f.* apêndice A), verificou-se que 72,6% dos estudantes considera o *Smartphone* muito útil para comunicar com a sua rede de contactos pessoais e 53% considera-o muito útil para a comunicação com a sua rede de contactos universitários. 52,1% avaliou igualmente muito útil a possibilidade de partilhar fotos, vídeos e ficheiros pelo *Smartphone*, havendo 90,9% a indicar que o seu trabalho se torna mais rápido com o uso do telemóvel. De um modo geral (81,7%), a eficiência, no seu trabalho de dia a dia, aumenta com a utilização do aparelho. Quando se pretendeu saber até que ponto os estudantes sentiam que o *Smartphone* afetava os seus estudos, constatou-se que se dividiam em dois grandes grupos: os que sentem que o *Smartphone* os afeta pouco (42,9%) e os que sentem que o *Smartphone* os afeta, pelo menos, bastante (38,2%). 36,6% dos estudantes, previamente a terem um *Smartphone*, considerava que o mesmo teria uma utilidade neutra e 35% considerava bastante útil.

Quanto ao grupo da intenção comportamental (*c.f.* apêndice A), detetou-se que 67,8% dos alunos pretende usar, sempre que possível, o *Smartphone* e 53,3% tem a intenção de aumentar o uso das suas ferramentas.

93,7% dos inquiridos costuma utilizar o *Smartphone* para partilhar dados e fotografias, 43,2% não o utiliza para monitorizar a sua atividade física e 63,4% também não utiliza o *GPS* do mesmo para a finalidade referida, tendo em conta a análise do grupo sobre o uso real (UR) (*c.f.* apêndice A).

Mediante esta análise (*c.f.* apêndice A), apontaram-se diversas vantagens ao uso do *Smartphone*, em várias ocasiões no dia-a-dia dos estudantes – nomeadamente, no uso académico, na comunicação e na partilha de dados.

Tendo por base os testes gerados com a variável sexo no *SPSS* (Tabela 28, *c.f.* apêndice B), ficou evidente uma indicação estatística de dependência e um grau de associação/correlação com os itens 22 (sempre teve certeza de como era a utilização do *Smartphone*), item 27 (Utiliza *Smartphone* para uso académico), item 35 (as ferramentas do *Smartphone* são flexíveis), item 41 (usar ferramentas do *Smartphone* o trabalho fica rápido), item 43 (*Smartphone* afeta os estudos), item 45 (quer utilizar *Smartphone*), item 46 (intenção de aumentar o uso das ferramentas do *Smartphone*), item 55 (costuma usar *Smartphone* para partilhar multimédia) e item 57 (usa *GPS* para atividades físicas e desportivas), com nível de relevância de 5% e 10%.

Averiguou-se a razão de chances (*odds ratio*) (Tabela 29, *c.f.* apêndice B), após o reconhecimento das variáveis associadas ao sexo. Mais uma vez, apenas as variáveis que mostraram ter dependência (χ^2), ter associação (*V*) e serem de natureza dicotômica (possuírem duas categorias) foram testadas, tendo apresentado significância estatística as que correspondem aos itens 22, 41, 45, 46, 55 e 57. Destaca-se que, relativamente às raparigas, os rapazes têm 70% mais de chances de ter a certeza de como era a utilização do *Smartphone*, têm uma possibilidade de aumentar o uso das ferramentas do mesmo duas vezes e meia superior (263%) e quase duas vezes mais probabilidades (183%) de usar o *GPS*, para atividade físicas e desportivas. Pelo contrário, o sexo masculino mostrou chances inferiores (menos 69%) no que diz respeito à ideia de que o uso das ferramentas deste telemóvel torna o trabalho mais rápido, no que remete para a vontade de usar este aparelho (menos 42%) e quanto à partilha de multimédia (menos 78%), comparativamente com o sexo feminino.

Graças aos testes aplicados com a variável geração, verificou-se (Tabela 30, *c.f.* apêndice B) a indicação de uma existência estatística de dependência e de um grau de associação/correlação com os itens 46 (intenção de aumentar o uso das ferramentas do *Smartphone*) e 57 (usa *GPS* para atividades físicas e desportivas), com nível de significância de 5% e 10%.

Denotou-se um grau de associação/correlação com o item 22 (Sempre teve certeza de como era a utilização do *Smartphone*), com nível de relevância de 5% e 10%, atendendo ao estudo dos testes gerados com a variável curso (Tabela 32, *c.f.* apêndice B).

4.2.22. Determinar a quantidade de utilização do *Smartphone*;

Neste ponto, avaliou-se um conjunto de 12 perguntas, criadas a partir do modelo *TUM*, utilizado neste estudo. Graças à ferramenta *SPSS*, fez-se uma análise estatística, após uma avaliação descritiva.

Tendo em conta as variáveis do grupo do perfil tecnológico (*c.f.* apêndice A), verificou-se que três terços dos estudantes (75,1%) estão, várias vezes por dia, online na sua aplicação preferida.

No grupo do uso do *Smartphone* (c.f. apêndice A), observou-se que os estudantes (99,1%), em média, utilizam o *Smartphone* todos os dias. A maioria (60,6%) gasta mais de três horas por dia no telemóvel e mais de metade (54,6%) utiliza-o entre 11 a 30 horas, por semana.

No grupo da utilidade percebida (c.f. apêndice A) do questionário, denotou-se que 90,9% dos estudantes indicou que o seu trabalho fica mais rápido, ao usar o *Smartphone*. 81,7% indicou que, com esse uso, a eficiência, no seu trabalho de dia-a-dia, aumenta. Relativamente ao grau de prejudicialidade nos estudos devido ao uso do *Smartphone*, os inquiridos estão divididos em dois grandes grupos: os que sentem que este aparelho os afeta pouco (42,9%) e os que sentem que o mesmo os afeta, pelo menos, bastante (38,2%). 36,6%, previamente a ter um *Smartphone*, considerava que a utilização deste teria uma utilidade neutra e 35% considerava que seria bastante útil.

No que remete para o grupo da intenção comportamental (c.f. apêndice A), constatou-se 67,8% dos alunos pretende, sempre que possível, usar o *Smartphone*. Quanto às ferramentas do mesmo, 53,3% tem a intenção de aumentar o seu uso, havendo 81,1% que adoraria ter inovações desse tipo, futuramente.

No que diz respeito à análise do grupo sobre o uso real (UR) (c.f. apêndice A), verificou-se que os estudantes (86,4%) utilizam as ferramentas do *Smartphone* todos dias.

Com a análise das questões que permitiram determinar a quantidade de uso por parte dos universitários, verificou-se que estão várias vezes online, por dia, na sua aplicação favorita, utilizando o *Smartphone*, diariamente, por mais de três horas. Um dos grandes pontos positivos deste dispositivo é o facto de ter vantagens no trabalho e nos estudos dos estudantes, razão pela qual as ferramentas deste telemóvel têm um uso diário por parte dos inquiridos.

Constatou-se a existência de uma indicação estatística de dependência e de um grau de associação/correlação com os itens 41 (usar ferramentas do *Smartphone* o trabalho fica rápido), 43 (*Smartphone* afeta os estudos), 45 (quer utilizar *Smartphone*), 46 (intenção de aumentar o uso das ferramentas do *Smartphone*) e 47 (adorava ter novas ferramentas no *Smartphone*), com nível de relevância de 5% e 10%, tendo por base os testes gerados no SPSS com a variável sexo (Tabela 32, c.f. apêndice B).

Depois de se apurarem as variáveis associadas ao sexo, averiguou-se a razão de chances (*odds ratio*), como pode ser observado (Tabela 33, *c.f.* apêndice B). Torna-se a evidenciar que, tal como em casos anteriores, apenas se testaram variáveis que mostraram ter dependência (χ^2), ter associação (*V*) e serem de natureza dicotômica (possuírem duas categorias), sendo os itens 41, 45, 46 e 47 aqueles que apresentaram significância estatística. Destaca-se que os rapazes têm 69% menos de chances de, ao usar ferramentas do *Smartphone*, o trabalho ficar mais rápido, e têm 42% menos de chances de querer utilizar este telemóvel sempre que possível, em relação às raparigas. Pelo contrário, o sexo masculino demonstrou ter uma possibilidade duas vezes e meia superior (263%) de aumentar o uso das suas ferramentas, assim como de adorar a aquisição de novas ferramentas (257%), comparativamente com o sexo feminino.

Através dos testes executados a partir da variável geração, verificou-se (Tabela 34, *c.f.* apêndice B) uma indicação da existência estatística de dependência e um grau de associação/correlação com o item 46 (intenção de aumentar o uso das ferramentas do *Smartphone*), com nível de significância de 5% e 10%.

Com o estudo dos testes previamente efetuados com a variável curso (Tabela 35, *c.f.* apêndice B), detetou-se a inexistência de um grau de associação/correlação, com nível de relevância de 5% ou 10%.

4.2.23. Determinar se o utilizador é *digitally savvy*;

Com a finalidade de dar uma resposta a este ponto, examinou-se um conjunto de 43 perguntas, criadas a partir do modelo *TUM*, utilizado neste estudo. Inicialmente, de forma descritiva e, de seguida, foi feita uma análise estatística, utilizando a ferramenta *SPSS*.

Tendo em conta as variáveis correspondentes ao grupo do perfil tecnológico (*c.f.* apêndice A), verificou-se que 94,3% dos estudantes utiliza o *Smartphone* há, pelo menos, quatro anos e que 75,1% está, várias vezes por dia, online na sua aplicação favorita. Além deste aspeto, constatou-se que 80,1% dos inquiridos tem o hábito de abrir e usar o equipamento, sem ler as instruções ou o manual de instruções, 66,9% sente que o *Smartphone* afeta os seus estudos, pelo menos, de uma forma ligeiramente positiva, 49,8% já teve um nível de dissonância, perante as expectativas de algumas funcionalidades, com a realidade, depois da utilização das mesmas e 62,5% indicou ter sempre a certeza de como era a utilização do telemóvel. Com 92,1% dos inquiridos a

possuir um *Smartphone* há mais de três anos, verificou-se que 90,5% acha que sempre o utilizou corretamente, havendo 90,9% a considerar que aprender a usá-lo é, pelo menos, bastante fácil, 69,4% a referir que a sua utilização requer pouco ou nenhum esforço mental e 72,6% a afirmar que é muito fácil comunicar com os seus contactos. 99,1% utiliza este aparelho diariamente – 60,6% indica, em média, estar mais de três horas, por dia, no seu telemóvel, e 57,1% utiliza-o, pelo menos, 21 horas, por semana -, mas apenas 67,8% refere que o pretende usar sempre que possível. Previamente a ter um *Smartphone*, 36,6% dos inquiridos considerava que este teria uma utilidade neutra para os seus estudos e 35% considerava que seria bastante útil no mesmo contexto. Atualmente, 95,6% utiliza-o para fins académicos, havendo 95,9% que sente que este aparelho os afeta nos estudos. A maioria de 90,9% indicou que o seu trabalho fica mais rápido com este uso e 81,7% aponta uma maior eficácia também devido a esse uso. As ferramentas são vistas, por 93,7%, como flexíveis, de forma a poderem usá-las da forma que melhor lhes convier, constatando-se que 60,9% considera fácil partilhar fotografias, vídeos e estados no *Smartphone* e 52,1% encara esta funcionalidade como algo útil. A interação com este telemóvel, é, pelo menos, bastante flexível, na opinião de 87,4% dos alunos. Quanto à comunicação com as suas redes de contactos, 72,6% considera-o muito útil para comunicar com contactos pessoais e 53% também o avalia dessa forma relativamente a contactos universitários. Mais de 40% dos estudantes utiliza este dispositivo para monitorizar a sua atividade física/desportiva e 36,6% costuma utilizar o *GPS* do seu *Smartphone* para essas atividades. No que toca à segurança, os universitários estão bastante divididos: uma parte sente-se mais segura e outra menos. Note-se que são muitos os alunos que sentem uma segurança neutra para partilhar conteúdos, comunicar com outros e jogar as mais diversas aplicações. 64% divulga informações pessoais no telemóvel.

Todos estes factos permitem verificar que a amostra se pode caracterizar como *digitally savvy*, visto que têm equipamentos de alta tecnologia, nos quais interagem, frequentemente, com a internet, e demonstram conhecimento de inúmeras ferramentas nos mesmos.

Tendo em conta os testes concebidos com a variável sexo no *SPSS* (Tabela 36, c.f. apêndice B), denotou-se uma indicação estatística de dependência e um grau de associação/correlação com os itens 22 (sempre teve a certeza de como era a utilização do *Smartphone*), item 27 (utiliza *Smartphone* para uso académico), item 34 (considera fácil

comunicar com os seus contactos), item 35 (as ferramentas do *Smartphone* são flexíveis), item 41 (usar ferramentas do *Smartphone* o trabalho fica rápido), item 41 (Ao usar ferramentas do *Smartphone* o trabalho fica mais rápido), item 43 (*Smartphone* afeta os estudos), item 45 (quer utilizar *Smartphone*) e item 57 (usa *GPS* para atividades físicas e desportivas) com nível de significância de 5% e 10%.

Reconhecidas as variáveis associadas ao sexo (*c.f.* apêndice B), averiguou-se a razão de possibilidades (*odds ratio*) (Tabela 37, *c.f.* apêndice B). Testaram-se, exclusivamente, as variáveis que tinham dependência (χ^2), associação (*V*) e que eram de natureza dicotómica (possuem duas categorias). As que apresentaram significância estatística correspondem aos itens 22, 41, 45 e 57. Em relação às raparigas, destaca-se que os rapazes têm 69% menos de chances de, ao usar ferramentas do *Smartphone*, o trabalho ficar mais rápido e têm 42% menos de possibilidades de o querer utilizar sempre que possam. No entanto, o sexo masculino tem 70% mais de certezas no que respeita à correta utilização do *Smartphone* e apresentam probabilidades 83% superiores relativamente ao uso do *GPS*, para atividades físicas e desportivas, comparativamente com o sexo feminino.

Com nível de relevância de 10%, verificou-se (Tabela 38, *c.f.* apêndice B) a indicação de uma existência estatística de dependência e de um grau de associação/correlação com o item 57 (usa *GPS* para atividades físicas e desportivas), tendo por base os testes gerados com a variável geração.

Com a consulta dos testes elaborados com a variável curso (Tabela 39, *c.f.* apêndice B), denotou-se uma associação/dependência com o item 22 (Sempre teve certeza de como era a utilização do *Smartphone*), item 36 (considera fácil partilhar multimídias), item 59 (considera seguro de partilhar multimídia) e item 60 (sente seguro para comunicar-se com contactos e empresa), com nível de significância de 5% ou 10%.

4.2.24. Determinar o tipo de informações que os utilizadores estão a fornecer às organizações que disponibilizam os serviços através dos *Smartphones*;

O conjunto de 22 perguntas elaboradas a partir do modelo *TUM*, utilizado neste estudo, foi tido em conta para este ponto, uma vez que foi analisado de forma descritiva e estatística, utilizando a ferramenta *SPSS*.

Com a recolha das variáveis do grupo do perfil tecnológico (*c.f.* apêndice A), observou-se que mais de metade dos alunos utiliza todas as aplicações tidas em conta para o estudo (câmara, *GPS*, Navegador *WEB*, calendário, e-mail, agenda de contactos, mensagens e chamadas). A maioria deles inclui, no seu perfil do *Smartphone*, o nome real (86,4%), endereço de e-mail (76,3%), número de telemóvel (63,1%) e fotografias pessoais (62,1%). A maior parte (74,8%) aceita os termos de utilização, ainda que estes impliquem a permissão do acesso aos dados de posicionamento do *Smartphone*.

Ao analisar as variáveis do grupo da teoria do nível de adaptação (*c.f.* apêndice A), denotou-se que 37,9% dos estudantes confiava pouco na partilha de informação inerente à utilização das aplicações necessárias ao funcionamento do *Smartphone* e 36,9% apresentava uma confiança mediana (confiança neutra). Verificou-se que 36,9% considerava, previamente a ter um *Smartphone*, que a sua utilização teria alguns riscos de privacidade, relativamente aos dados móveis que partilharia. O estudo também mostra que 30% dos inquiridos considerava que a utilização da câmara do *Smartphone* oferecia poucos riscos de segurança e 33,8% não apontava qualquer necessidade de instalar uma aplicação para manter o seu direito à privacidade, quando utiliza o telemóvel.

No grupo da intenção comportamental (*c.f.* apêndice A), verificou-se que 70,7% dos estudantes indicou não sentir a necessidade de tapar a câmara do *Smartphone*, em algumas situações, e 58,4% tem a necessidade de desligar o *GPS* no telemóvel, sempre que não precisa dele. A grande maioria dos universitários (92,4%) também não sente a necessidade de desligar o *Smartphone* por completo durante os períodos em que não o está a utilizar, por questões de segurança. 59,3% dos inquiridos não tem a intenção de adquirir uma aplicação para se defender da invasão de terceiros e 58% adorava ter um botão que permitisse ligar e desligar o microfone do seu *Smartphone*.

Na análise às variáveis do grupo sobre o uso real (UR) (*c.f.* apêndice A), observou-se que, de todas as funcionalidades apresentadas aos inquiridos (Páginas *WEB*, *GPS*, calendário, e-mail, contactos, câmaras, microfone, mensagens), apenas o microfone não é utilizado por, pelo menos, metade dos estudantes. 86,4% utiliza o *Smartphone* todos dias e 93,7% costuma usá-lo para partilhar dados e fotografias. 56,8% não utiliza o telemóvel para monitorizar a sua atividade física/desportiva, havendo 63,4% que também não utiliza o *GPS*, no seu *Smartphone*, com a mesma finalidade.

Em relação ao grupo da confiança e segurança do questionário (*c.f.* apêndice A), constatou-se que a grande maioria dos estudantes (64%) divulga as suas informações pessoais no *Smartphone*. Quanto à partilha de fotografias, vídeos, ficheiros e informações pessoais, 47,6% considera o *Smartphone* medianamente seguro (segurança neutra) e 28,7% considera pouco seguro. No que toca à utilização do *Smartphone* para comunicar com os seus contactos ou empresas, 43,5% sente-se medianamente seguro (segurança neutra) e 33,8% sente-se bastante seguro. Em relação à questão que procurava saber se os estudantes se sentem seguros ao utilizar o *Smartphone* para jogar as mais diversas aplicações, 41,3% dos inquiridos indicou que se sente mais ou menos seguro (segurança neutra) e 29,3% indicou que se sente bastante seguro. Na questão que pretendia saber se os estudantes se sentem seguros ao utilizar o telemóvel para ter conversas privadas relacionadas com trabalho ou dados sensíveis, 40,1% sente-se medianamente seguro e 24,3% bastante seguro.

Com a análise dos dados, verificou-se que a maior parte dos alunos introduz uma grande variedade de dados privados no *Smartphone*, os quais permitem identificar o indivíduo, a sua rede de contactos, os seus dados de posicionamento, as suas fotografias pessoais e muitos outros, dependendo do tipo de comunicação de cada um, através do dispositivo (seja uma comunicação com a sua rede de contactos ou uma pesquisa na internet). Os inquiridos afirmaram ter alguma insegurança, não sabendo se devem confiar ao dispositivo os seus dados, mas o comportamento dos mesmos mostra que a confiança é suficiente para partilharem os seus dados privados, através do seu telemóvel. Verificou-se também que os utilizadores permitem que o seu *Smartphone* tenha acesso a uma elevada quantidade de dados.

Com os testes produzidos com a variável sexo no *SPSS*, verificou-se (Tabela 40, *c.f.* apêndice B) que existe uma indicação estatística de dependência e um grau de associação/correlação com os itens 12 (aceita termos de aceitação), item 15 (confia a partilha de informação), item 16 (utilização do mesmo tem risco aos dados móveis), item 18 (instalar um aplicação para manter a privacidade), item 48 (necessidade de tapar a câmara do *Smartphone*), item 50 (desligar o *Smartphone* no momento que não utiliza), item 55 (costuma usar *Smartphone* para partilhar multimídia) e item 57 (usa *GPS* para atividades físicas e desportivas), com nível de relevância de 5% e 10%.

Com o propósito de averiguar a razão de chances (*odds ratio*) (Tabela 41, *c.f.* apêndice B), depois de apurar as variáveis associadas ao sexo, testaram-se as que mostraram ter dependência (χ^2), ter associação (*V*) e serem de natureza dicotômica (possuírem duas categorias), tendo apresentado significância estatística os itens 12, 48, 50, 55, 57. Denotou-se que os rapazes têm mais de o dobro (212%) de chances de consentir com os termos de aceitação, quando estes implicam um acesso aos dados de posicionamento do *Smartphone*, assim como têm 83% mais de chances de usar *GPS* para atividades físicas e desportivas, em relação às raparigas. No entanto, comparativamente com o sexo feminino, o masculino tem 74% menos de possibilidades de tapar a câmara do *Smartphone* e apresenta uma probabilidade inferior a três quartos (22%) de ter o hábito de o utilizar para partilhar multimédia.

Apresentando um nível significância de 5% e 10%, verificou-se (Tabela 42, *c.f.* apêndice B) uma existência estatística de dependência e um grau de associação/correlação com os itens 15 (confia a partilha de informação), 17 (Utilização da câmara tem risco de segurança), 18 (Instalar uma aplicação para manter a privacidade), 57 (Usa *GPS* para atividades físicas e desportivas), com base nos testes com a variável geração.

Tendo em conta a análise dos testes concebidos com a variável curso (Tabela 43, *c.f.* apêndice B), denotou-se uma associação/dependência com os itens 59 (considera seguro de partilhar multimédia) e item 60 (sente-se seguro para comunicar com contactos e empresa), sendo o nível de relevância de 5% ou 10%.

4.2.25. Determinar se a população estudada sabe que tipo de informações está a disponibilizar a terceiros, ao usar o seu telemóvel;

Neste contexto, foi analisado um conjunto de 22 perguntas, concebidas graças ao modelo *TUM*, utilizado neste estudo. Primeiro, de forma descritiva e, posteriormente, com o auxílio da ferramenta *SPSS*, fez-se uma análise estatística.

Observando as variáveis do grupo do perfil tecnológico (*c.f.* apêndice A), constatou-se que a maior parte dos estudantes afirma ter conhecimento de que terceiros possam utilizar os dados pessoais registados pelo *Smartphone* (74,1%) e consente com os termos de aceitação, quando estes implicam um acesso aos dados de posicionamento do telemóvel (74,8%). Os dados introduzidos mais comuns são o nome real (86,4%), endereço de e-mail (76,3%), número de telefone (63,1%) e fotografias pessoais (62,1%).

Tendo por base as variáveis do grupo da teoria do nível de adaptação, denotou-se que, previamente a ter um *Smartphone*, 32,2% dos inquiridos considerava que a utilização das aplicações de comunicação teria riscos para a sua privacidade e 36% acreditava que o uso do telemóvel teria alguns riscos de privacidade, relativamente aos dados móveis que partilharia. Ainda previamente à obtenção deste telemóvel, 37,9% afirmou que teria pouca confiança na partilha de informação inerente à utilização das aplicações necessárias ao funcionamento do aparelho e 36,9% referiu que teria uma confiança mediana. O estudo também mostra que 30% considerava pouco arriscado o uso da câmara do *Smartphone* e 33,8% não achou nada necessária a instalação de uma aplicação para manter o seu direito à privacidade, quando o utiliza.

Na análise das variáveis do grupo da teoria da dissonância cognitiva (*c.f.* apêndice A), verificou-se que a maioria dos universitários (77,9%) já teve momentos de preocupação no que respeita à sua privacidade, ao utilizar o *Smartphone*. 80,8% indicou que confiava no seu telemóvel, 94,6% sentiu-se confortável ao utilizá-lo e 96,5% afirmou que não vai deixar de o usar, mesmo sabendo quais os riscos de segurança associados a este equipamento.

Sobre o grupo da intenção comportamental (*c.f.* apêndice A), apurou-se que a maior parte dos inquiridos não sente a necessidade de tapar a câmara do *Smartphone*, em algumas situações (79,7%), assim como não vê qualquer necessidade de desligar o telemóvel por completo, durante os períodos em que não o utiliza, por questões de segurança (92,4%). No entanto, 58,4% revelou que necessita de desligar o *GPS* neste dispositivo, sempre que não precisa dele. 59,3% indicou que não tem a intenção de adquirir uma aplicação para se defender da invasão de terceiros e 58% adorava ter um botão que permitisse ligar e desligar o microfone do seu *Smartphone*.

No que remete para o grupo da confiança e segurança (*c.f.* apêndice A), verificou-se que a grande maioria dos estudantes (64%) divulga as suas informações pessoais no *Smartphone*. Em relação à partilha de fotografias, vídeos, ficheiros e informações pessoais, 47,6% considera este telemóvel medianamente seguro (segurança neutra) e 28,7% considera-o pouco seguro. No que diz respeito à utilização do *Smartphone* para comunicar com os seus contactos ou empresas, 43,5% sente-se medianamente seguro e 33,8% sente-se bastante seguro. Em relação à questão que pretende saber se os estudantes se sentem seguros ao utilizar o *Smartphone* para jogar as mais diversas aplicações, 41,3%

indicou que sente uma segurança intermédia (segurança neutra) e 29,3% indicou que se sente bastante seguro. Na questão que procura avaliar se os estudantes se sentem seguros ao utilizar o *Smartphone* para ter conversas privadas relacionadas com trabalho ou dados sensíveis, 40,1% considera que se sente medianamente seguro (segurança neutra) e 24,3% que se sente bastante seguro.

Com a análise dos dados que permitem responder a esta questão de investigação (c.f. apêndice A), denotou-se que os alunos partilham muitos dados no seu *Smartphone*. No entanto, parecem sentir-se inseguros relativamente aos que possam partilhar sem saber. Isto verificou-se, sobretudo, graças ao facto de alguns estudantes já terem sentido a necessidade de tapar a câmara, em algumas situações, de a maioria desligar o *GPS*, quando não o está a utilizar, e de a maior parte indicar que adoraria ter um botão que desligasse o microfone do *Smartphone*.

Detetou-se, com nível de relevância de 5% e 10%, uma indicação estatística de dependência e um grau de associação/correlação com os itens 12 (aceita termos de aceitação), item 15 (confia a partilha de informação), item 16 (utilização do mesmo tem risco aos dados móveis), item 18 (instalar um aplicação para manter a privacidade), 19 (houve alturas em que se preocupou com a privacidade), 23 (Confia no *Smartphone*), 24 (Sente-se confortável ao usar o *Smartphone*), 48 (Necessidade de tapar a câmara do *Smartphone*) e item 50 (Desligar o *Smartphone* no momento que não utiliza), partindo dos testes com a variável sexo, gerados no *SPSS*.

Conferidas as variáveis associadas ao sexo, investigou-se a razão de chances (*odds ratio*) (Tabela 45, c.f. apêndice B). Ressalta-se, novamente, que as únicas variáveis testadas foram as que mostraram ter dependência (χ^2), ter associação (*V*) e serem de natureza dicotómica (possuírem duas categorias), tendo apresentado significância estatística os itens 12, 19, 23, 48 e 50. Os rapazes têm mais de o dobro de chances de aprovar os termos de aceitação, quando estes implicam um acesso aos dados de posicionamento do *Smartphone* (212%), assim como de confiar no seu telemóvel (209%), em relação às raparigas. Também eles têm uma chance três vezes e meia (357%) maior de desligar o *Smartphone*, quando não o utilizam. Pelo contrário, o sexo masculino apresentou possibilidades 50% inferiores relativamente a ter momentos de preocupação com a sua privacidade durante o uso deste telemóvel e no que toca a tapar a câmara do *Smartphone* (74%) em relação às raparigas.

Os testes criados tendo por base a variável geração (Tabela 46, *c.f.* apêndice B) permitiram denotar uma existência estatística de dependência e um grau de associação/correlação com os itens 11 (terceiros utilizam os dados), 15 (confia a partilha de informação), 17 (Utilização da câmara tem risco de segurança), 18 (Instalar uma aplicação para manter a privacidade) e 26 (conhecendo os riscos de segurança, para de usar *Smartphone*), com nível de significância de 5% e 10%.

Denotou-se, também, uma associação/dependência com os itens 24 (sente-se confortável ao usar o *Smartphone*), item 59 (considera seguro de partilhar multimédia) e item 60 (sente-se seguro para comunicar com contactos e empresa), com o mesmo nível de significância, atendendo à análise dos testes concebidos com a variável curso (Tabela 47, *c.f.* apêndice B).

4.2.26. Compreender e identificar se é preciso tomar medidas futuras, de forma a proteger a privacidade digital de cada utilizador, para garantir uma utilização dos *Smartphones* que deixe os utilizadores sem medo de expor a sua privacidade;

Neste âmbito, de forma descritiva, analisou-se um conjunto de 12 perguntas, concebidas a partir do modelo *TUM*, aplicado no estudo. Posteriormente, procedeu-se a uma análise estatística, utilizando a ferramenta *SPSS*.

Avaliando as variáveis do grupo da teoria da dissonância cognitiva (*c.f.* apêndice A), observou-se que os estudantes, na sua grande maioria, já tiveram momentos durante os quais se preocuparam com a sua privacidade, ao utilizar o *Smartphone* (77,9%), embora não queiram deixar de se servir do mesmo, ainda que saibam quais os riscos de segurança associados a este equipamento (96,5%). A maior parte indicou confiar no seu telemóvel (80,2%) e também se sentiu confortável com o seu uso (94,6%). 96,2%, se pudesse voltar atrás, tornaria a comprar um *Smartphone*.

Sobre o grupo da intenção comportamental (*c.f.* apêndice A), constatou-se que 53,5% dos inquiridos tenciona aumentar o uso das ferramentas do *Smartphone* e 81,1% adorava ter ferramentas novas no mesmo. Apesar de a maioria dos universitários não ter a intenção de adquirir uma aplicação para se defender da invasão de terceiros (59,3%), gostaria de ter um botão que permitisse ligar e desligar o microfone (58%). Em períodos de inatividade e por questões de segurança, 92,4% não demonstrou necessidade de desligar o *Smartphone*, assim como 70,7% indicou não ter necessidade de tapar a câmara, em

algumas situações. No entanto, 58,4% tem a necessidade de desligar o *GPS* no *Smartphone*, sempre que não precisa dele.

Com a análise dos dados que permitem responder a esta pergunta de investigação, verificou-se que os alunos não pretendem deixar de utilizar o *Smartphone*, mesmo tendo conhecimento dos riscos de segurança para a sua privacidade, o que indica que as organizações não precisam de se preocupar muito em perder clientes, caso recolham e utilizem os dados dos utilizadores. Por vezes, os estudantes têm algumas incertezas no que respeita à segurança dos *Smartphones*, mas esse aspeto não parece ser o suficiente para tomarem medidas de proteção.

Com nível de relevância de 5% e 10%, graças aos testes concebidos com a variável sexo no *SPSS* (Tabela 48, *c.f.* apêndice B), constatou-se uma indicação estatística de dependência e um grau de associação/correlação com os itens 19 (houve alturas em que se preocupou com a privacidade), 20 (Não comprava um *Smartphone* se voltasse atrás), 23 (Confia no *Smartphone*), 24 (Sente-se confortável ao usar o *Smartphone*), 46 (Intenção de aumentar o uso das ferramentas do *Smartphone*), 47 (Adorava ter novas ferramentas no *Smartphone*), 48 (Necessidade de tapar a câmara do *Smartphone*) e item 50 (Desligar o *Smartphone* no momento que não utiliza).

Como se observa (Tabela 49, *c.f.* apêndice B), uma vez identificadas as variáveis associadas ao sexo, averiguou-se a razão de chances (*odds ratio*), testando apenas as que mostraram ter dependência (χ^2), ter associação (*V*) e serem de natureza dicotómica (possuírem duas categorias). As que apresentaram significância estatística correspondem aos itens 19, 23, 46, 47, 48 e 50. Os rapazes, em relação às raparigas, têm metade das chances de ter momentos de preocupação com a sua privacidade, ao utilizar o *Smartphone*. Também eles têm duas vezes e meia mais de chances (263%) de tencionar aumentar as ferramentas deste dispositivo e igualmente mais duas vezes e meia (257%) de adorar ter novas ferramentas no mesmo. O sexo masculino apresenta possibilidades superiores no que respeita à confiança no telemóvel (209%) e relativamente ao facto de o desligar quando não o usa (357%). No entanto, tem 74% menos de chances de tapar a câmara do *Smartphone*, comparativamente com o sexo feminino.

Com um nível de relevância de 5% e 10%, observou-se (Tabela 50, *c.f.* apêndice B) a indicação de uma existência estatística de dependência e de um grau de

associação/correlação com os itens 26 (conhecendo os riscos de segurança, para de usar *Smartphone*) e 46 (intenção de aumentar o uso das ferramentas do *Smartphone*), através dos testes concebidos com a variável geração.

Mediante os testes gerados com a variável curso (Tabela 51), denotou-se uma associação com o item 24 (sente-se confortável ao usar o *Smartphone*), com nível de significância de 5% ou 10%.

4.2.27. Perceber que utilização as pessoas fazem dos seus dispositivos móveis;

Com o propósito de responder a esta questão, realizou-se uma análise estatística, utilizando a ferramenta *SPSS*, depois de uma avaliação de um conjunto de 48 perguntas, elaboradas a partir do modelo *TUM*, utilizado no estudo.

Devido à investigação do grupo do perfil tecnológico (*c.f.* apêndice A), verificou-se que a maior parte dos inquiridos se liga à internet através da rede de casa (96,8%), da rede da sua operadora (76,7%) e através de redes Wi-Fi em lugares públicos (57,7%), com o propósito de participar nas redes sociais (87,4%), ver vídeos (81,1%), pesquisar conteúdos (73,5%), navegar nas páginas da Internet (73,2%) e consultar o e-mail (71,9%). As aplicações do *Smartphone* analisadas neste estudo são utilizadas, pelo menos, por mais de metade dos estudantes: aplicação de mensagens (98,1%), aplicação de chamadas (95%), aplicação da câmara (94,6%), aplicação do e-mail (92,1%), aplicação para navegar na internet (*Web Browser*) (89%), aplicação com *GPS* (87,4%), aplicação do calendário (72,6%) e aplicação da agenda de contactos (65,6%). A maioria dos alunos (94,4%) tem um *Smartphone* há, pelo menos, quatro anos, estando várias vezes, por dia, online, na sua aplicação favorita (75,1%). A maior parte inclui o nome real (86,4%) no perfil da conta do seu telemóvel, o endereço de e-mail (76,3%), o número de telemóvel/telefone (63,1%) e fotografias pessoais (62,1%). 80,1% dos alunos tem o hábito de abrir e usar o equipamento, sem ler as instruções ou o manual de instruções, e 41% sente que este aparelho afeta de uma forma ligeiramente negativa.

Com a apreciação das variáveis do grupo da teoria da dissonância cognitiva (*c.f.* apêndice A), constatou-se que os estudantes, na sua grande maioria (77,9%), já tiveram momentos de preocupação com a sua privacidade, ao utilizar o *Smartphone*. 80,8% indicou que confiava no seu telemóvel, 94,6% sentiu-se confortável com a sua utilização e 90,5% indicou que não o utilizou corretamente.

No grupo do uso do *Smartphone* (c.f. apêndice A), verificou-se que 95,6% utiliza o telemóvel para fins académicos, havendo 99,1% que o utiliza diariamente. A maioria dos universitários (60,6%) indica, em média, estar mais de três horas, por dia, no seu *Smartphone*. 92,1% indica que possui um destes aparelhos há mais de três anos e 57,1% referiu que, por semana, utiliza-o, pelo menos, 21 horas

Na facilidade percebida (c.f. apêndice A), a maioria dos estudantes (90,9%) considera que aprender a utilizar o *Smartphone* é, pelo menos, bastante fácil. 69,4% considera que a sua utilização requer pouco ou nenhum esforço mental e 72,6% considera muito fácil comunicar com os seus contactos. 93,7% vê as ferramentas como flexíveis, de forma a poder usá-las da melhor forma e 60,9% considera fácil partilhar fotografias, vídeos e estados no *Smartphone*. Os alunos (87,4%) consideram que a interação com este dispositivo é, pelo menos, bastante flexível.

Quanto ao grupo da utilidade percebida do questionário (c.f. apêndice A), observou-se que 72,6% dos inquiridos considera o *Smartphone* muito útil para comunicar com a sua rede de contactos pessoais e que 53% o considera muito útil na comunicação com a sua rede de contactos universitários. 52,1% considera igualmente muito útil a possibilidade de partilhar fotos, vídeos e ficheiros pelo *Smartphone*. 90,9% indicou que o seu trabalho fica mais rápido com esta utilização e 81,7% apontou que a mesma também aumenta a sua eficiência no trabalho. Nos estudos, 42,9% sente que o *Smartphone* os afeta pouco e 38,2% sente que os afeta, pelo menos, bastante, o que permite verificar a existência de dois grandes grupos. Previamente a terem um *Smartphone*, 36,6% considerava que a sua utilização teria uma utilidade neutra e 35% considerava que seria bastante útil.

Sobre o grupo da intenção comportamental (c.f. apêndice A), denotou-se que 67,8% pretende usar, sempre que possível, o *Smartphone*, havendo 92,4% que não vê a necessidade de o desligar, durante os períodos em que não o usa, por questões de segurança. 70,7% indicou não ter a necessidade de tapar a câmara, em algumas situações, mas 58,4% afirmou ter a necessidade de desligar o *GPS* no *Smartphone*, sempre que não precisa dele. 81,1% manifestou vontade de adquirir novas ferramentas no seu telemóvel e 53,5% tenciona aumentar o uso das mesmas. Apesar de 58% gostar da ideia de ter um botão que permita ligar e desligar o microfone, 59,3% não tenciona adquirir uma aplicação para se defender da invasão de terceiros.

Na análise às variáveis do grupo sobre o uso real (UR) (*c.f.* apêndice A), apurou-se que, de todas as funcionalidades apresentadas (Páginas *WEB*, *GPS*, calendário, e-mail, contactos, câmaras, microfone, mensagens) aos inquiridos, apenas o microfone não é utilizado por, pelo menos, metade dos estudantes. 86,4% utiliza as ferramentas do *Smartphone* todos dias e 93,7% costuma usá-lo para partilhar dados e fotografias. 56,8% não utiliza o *Smartphone* para monitorizar a sua atividade física/desportiva e 63,4% também não utiliza o *GPS* no seu *Smartphone*, para a mesma finalidade.

Em relação ao grupo da confiança e segurança do questionário (*c.f.* apêndice A), comprovou-se que a maior parte dos alunos (64%) divulga as suas informações pessoais no *Smartphone*. Em relação à partilha de fotografias, vídeos, ficheiros e informações pessoais, 47,6% considera este aparelho medianamente seguro (segurança neutra) e 28,7% considera-o pouco seguro. No que toca à utilização do telemóvel para comunicar com os seus contactos ou empresas, 43,5% sente-se medianamente seguro (segurança neutra) e 33,8% sente-se bastante seguro. 41,3% indicou sentir-se mais ou menos seguro (segurança neutra) ao utilizar o *Smartphone* para jogar as mais diversas aplicações e 29,3% indicou sentir-se bastante seguro para o mesmo efeito. Na questão que procura saber o nível de segurança dos inquiridos ao utilizar este aparelho para ter conversas privadas relacionadas com trabalho ou dados sensíveis, 40,1% considera que se sente medianamente seguro (segurança neutra) e 24,3% respondeu que se sente bastante seguro.

Verificou-se que os estudantes têm uma grande utilização do *Smartphone* e das suas respetivas ferramentas, utilizando o equipamento, nas várias situações do seu dia-a-dia, para os mais diversos fins. Tal comportamento demonstrou-nos que estes têm por hábito expor o *Smartphone* a todo o tipo de situações, sejam privadas ou não.

Com o auxílio dos testes criados com a variável sexo no *SPSS*, verificou-se (Tabela 52, *c.f.* apêndice B) que existe uma indicação estatística de dependência e um grau de associação/correlação com os itens 19 (houve alturas em que se preocupou com a privacidade), 23 (Confia no *Smartphone*), 24 (Sente-se confortável ao usar o *Smartphone*), 27 (Utiliza *Smartphone* para uso académico), 41 (Usar ferramentas do *Smartphone* o trabalho fica rápido), 43 (*Smartphone* afeta os estudos), 45 (Quer utilizar *Smartphone*), 46 (Intenção de aumentar o uso das ferramentas do *Smartphone*), 47 (Adorava ter novas ferramentas no *Smartphone*), 48 (Necessidade de tapar a câmara do *Smartphone*), item 50 (Desligar o *Smartphone* no momento que não utiliza), 55 (Costuma

usar *Smartphone* para partilhar multimídia) e 57 (Usa GPS para atividades físicas e desportivas), com nível de significância de 5% e 10%.

Mais uma vez, averiguou-se a razão de chances (*odds ratio*) (Tabela 53, *c.f.* apêndice B), depois de examinadas as variáveis associadas ao sexo. Tendo em conta que se testaram apenas as variáveis que mostraram ter dependência (χ^2), ter associação (V) e serem de natureza dicotómica (possuírem duas categorias), os itens 19, 23, 41, 45, 46, 47, 48, 50, 55 e 57 foram os que apresentaram relevância estatística. Os rapazes têm metade das chances de ter fases de preocupação com a sua privacidade, ao utilizar o *Smartphone*, têm hipóteses inferiores a dois terços (31%) de usar ferramentas no telemóvel e do seu trabalho ficar mais rápido, têm quase metade das probabilidades (58%) de querer utilizar, sempre que possível, este aparelho, têm 74% menos chances de tapar a câmara do *Smartphone* e têm menos de três quartos (22%) de possibilidades de ter o hábito de o usar para partilhar multimédia, em relação às raparigas. Pelo contrário, o sexo masculino apresenta duas vezes mais (209%) de chances de confiar no *Smartphone*, assim como de ter a intenção de aumentar as ferramentas do mesmo (263%) e de adorar essas novas ferramentas (257%). É também o sexo masculino que tem mais de três vezes e meia (357%) de chances de sentir a necessidade de desligar o telemóvel, quando não o utiliza, e que denota mais 83% de possibilidades de usar o *GPS* para atividades físicas/desportivas, em relação ao sexo feminino.

Através dos testes concebidos com a variável geração, verificou-se (Tabela 54, *c.f.* apêndice B) a indicação de uma existência estatística de dependência e de um grau de associação/correlação com os itens 46 (intenção de aumentar o uso das ferramentas do *Smartphone*) e 57 (Usa *GPS* para atividades físicas e desportivas), com nível de relevância de 5% e 10%.

Observou-se uma associação com os itens 24 (sente-se confortável ao usar o *Smartphone*), 36 (Considera fácil partilhar multimídias), 59 (Considera seguro de partilhar multimídia), 60 (Sente-se seguro para comunicar com contactos e empresa), com nível de significância de 5% ou 10%, através do estudo dos testes elaborados com a variável curso (Tabela 55).

4.2.28. Determinar se a população aceita ter uma vida digital transparente no futuro;

Neste contexto, analisou-se de forma descritiva um conjunto de 17 perguntas, criadas a partir do modelo *TUM*, utilizado neste estudo. Posteriormente, com o auxílio da ferramenta *SPSS*, fez-se uma análise estatística.

No estudo das variáveis do grupo da teoria da dissonância cognitiva (*c.f.* apêndice A), verificou-se que os alunos, na sua grande maioria, já tiveram momentos de preocupação com a sua privacidade, ao utilizar o *Smartphone* (77,9%), apesar de não deixarem de o usar, ainda que saibam quais os riscos de segurança associados ao mesmo (96,5%). 62,5% sempre teve a certeza de como era a utilização do *Smartphone* e 96,2%, se pudesse voltar atrás, voltaria a comprá-lo. 50,2% dos inquiridos apresentou uma inconsistência entre as expectativas antes da utilização e a realidade das funcionalidades do telemóvel depois de o utilizar.

No que diz respeito ao grupo da intenção comportamental (*c.f.* apêndice A), constatou-se que, por questões de segurança, 92,4% dos inquiridos não desliga o *Smartphone* em períodos de inatividade, havendo 67,8% que pretende usá-lo sempre que possível. A intenção de aumentar o uso das ferramentas do telemóvel foi manifestada por 53,3% dos universitários. 59,3% não pretende adquirir uma aplicação para se defender da invasão de terceiros, mas 58% adorava ter um botão que permitisse ligar e desligar o microfone. Apesar de 58,4% ter a necessidade de desligar o *GPS* neste aparelho, sempre que não precisa dele, 70,7% não necessita de tapar a câmara, em algumas situações.

Em relação ao grupo da confiança e segurança do questionário (*c.f.* apêndice A), verificou-se que a grande maioria dos estudantes (64%) divulga as suas informações pessoais no *Smartphone*. A partilha de fotografias, vídeos, ficheiros e informações pessoais, através do telemóvel, é considerada medianamente segura (segurança neutra) por 47,6% e pouco segura por 28,7%. Quanto à utilização do *Smartphone* para comunicar com os seus contactos ou empresas, 43,5% sente-se medianamente seguro (segurança neutra) e 33,8% sente-se bastante seguro. O uso do dispositivo para jogar as mais diversas aplicações deixa 41,3% medianamente seguro (segurança neutra) e 29,3% indicou sentir-se bastante seguro com esse aspeto. 40,1% considera que se sente medianamente seguro

(segurança neutra), ao utilizar este telemóvel para conversas privadas relacionadas com trabalho ou dados sensíveis e 24,3% sente-se bastante seguro, no mesmo contexto.

Observou-se, tendo por base os testes concebidos com a variável sexo no *SPSS* (Tabela 56 *c.f.* apêndice B), que existe a indicação de uma estatística de dependência e de um grau de associação/correlação com os itens 19 (houve alturas em que se preocupou com a privacidade), 20 (Não comprava um *Smartphone* se voltasse atrás), 22 (Sempre teve certeza de como era a utilização do *Smartphone*), 45 (Quer utilizar *Smartphone*), 46 (Intenção de aumentar o uso das ferramentas do *Smartphone*), 48 (Necessidade de tapar a câmara do *Smartphone*) e item 50 (Desligar o *Smartphone* no momento que não utiliza), com nível de significância de 5% e 10%.

Reconhecidas as variáveis associadas ao sexo, avaliou-se a razão de chances (*odds ratio*) (Tabela 57, *c.f.* apêndice B). Ressalta-se que as únicas variáveis testadas foram as que mostraram ter dependência (χ^2), ter associação (*V*) e serem de natureza dicotómica (possuírem duas categorias), tendo os itens 19, 22, 45, 46, 48 e 50 manifestado uma relevância estatística. Os rapazes, comparativamente com as raparigas, têm metade das chances de ter momentos nos quais se preocuparam com a sua privacidade, ao utilizar o *Smartphone*, e têm quase metade (58%) de hipóteses de o querer usar, sempre que possível. São também eles que apresentam 74% menos de chances de tapar a câmara do mesmo. No entanto, o sexo masculino, por contraste com o feminino, denota duas vezes mais (70%) de probabilidades de sempre ter tido a certeza de como era a utilização do *Smartphone*, assim como apresenta uma intenção de aumentar as ferramentas do mesmo duas vezes e meia superior (263%). É igualmente o sexo masculino que tem mais de três vezes e meia (357%) de chances de sentir a necessidade de desligar o telemóvel, quando não o utiliza.

Mediante os testes realizados com a variável geração, constatou-se (Tabela 58, *c.f.* apêndice B), com nível de relevância de 5% e 10%, uma estatística de dependência e um grau de associação/correlação com os itens 26 (Conhecendo os riscos de segurança, para de usar *Smartphone*) e 46 (Intenção de aumentar o uso das ferramentas do *Smartphone*).

Graças aos testes gerados com a variável curso (Tabela 59, *c.f.* apêndice B), verificou-se uma associação/correlação com o item 22 (Sempre teve certeza de como era a utilização do *Smartphone*) e uma associação com os itens 24 (sente-se confortável ao usar

o *Smartphone*), 59 (Considera seguro de compartilhar multimídia) e 60 (Sente-se seguro para comunicar com contactos e empresa), com nível de significância de 5% ou 10%.

Apêndice D – Alpha de Cronbach

O coeficiente de *alpha de Cronbach* é estimado com base na equação apresentada na figura 16. Apesar de não haver um único valor que seja capaz de determinar, de forma consensual, quando é que esse coeficiente pode ser considerado bom, os valores de $\alpha \geq 0,600$, normalmente, são considerados satisfatórios, nomeadamente para estudos exploratórios. No entanto, com base nesta pesquisa, o *Alpha de Cronbach* (α) calculado para os itens dicotômicos (são 26) foi de 46,00% ($\alpha = 0,46$) e para os itens politômicos foi de 58,00% ($\alpha = 0,576$), sendo considerado razoável pela maioria das escalas (Domingos Silva Júnior & José Costa, 2014; Hair Jr. et al., 2006; Landis & Koch, 1977).

$$\alpha = \frac{k}{k-1} \left(\frac{\sum_{i=1}^k \sigma_i^2}{\sigma_y^2} \right)$$

Figura 16 - Formula modelo da aceitação

Fonte: (Gil, 2008)

Onde,

k: é o número de itens do questionário;

σ_i^2 : é a variância do item i;

σ_y^2 : É a variância da escala total somada.

O autor Gil (2008) destaca que o *Alpha de Cronbach* (α) é um dos coeficientes mais utilizados para avaliação de fidedignidade, ou seja, estabilidade, confiabilidade, consistência. Assim sendo, a consistência interna do instrumento possibilita avaliar o quanto as variáveis do mesmo valor relacional são inter-relacionadas entre si, sendo, assim, capazes de exprimir se as relações observadas são, de facto, coerentes. Então, quando se obtêm níveis adequados de coerência interna, espera-se que os resultados sejam igualmente coerentes e se repitam quando os mesmos instrumentos forem aplicados à mesma amostra.

Grupo 2		Grupo 7	
Itens Dicotômicos	Itens Politômicas	Itens Dicotômicos	Itens Politômicas
$\alpha = 0.074$	0	$\alpha = 0.597$	$\alpha = 0.476$
Grupo 3		Grupo 8	
Itens Dicotômicos	Itens Politômicas	Itens Dicotômicos	Itens Politômicas
0	$\alpha = 0.543$	$\alpha = 0.495$	0
Grupo 4		Grupo 9	
Itens Dicotômicos	Itens Politômicas	Itens Dicotômicos	Itens Politômicas
$\alpha = 0.139$	0	$\alpha = 0.518$	0
Grupo 6		Grupo 10	
Itens Dicotômicos	Itens Politômicas	Itens Dicotômicos	Itens Politômicas
-*	$\alpha = 0.376$	-*	$\alpha = 0.755$

* Número de itens insuficiente para o cálculo do coeficiente de fiabilidade (-).

Tabela 60 - Consistência Interna do Questionário pelo Alpha de Cronbach (α)

Apêndice E – Guião da Entrevista

Guião da Entrevista

Guião para entrevistas relacionadas com o tema “A privacidade dos dados pessoais na era dos *Smartphones*”

Introdução sobre o tema: Olá, o meu nome é Bruno Oliveira. Muito obrigado por virem fazer a entrevista para o meu estudo. Estou a fazer uma dissertação, aqui, no ISCTE-IUL, sobre a privacidade dos dados pessoais, na era dos *Smartphones*, entre estudantes universitários.

Objetivo da entrevista: O objetivo desta entrevista é perceber se os estudantes universitários do primeiro ano da escola ISTA do ISCTE-IUL sabem que a sua privacidade pessoal está em risco, quando usam o *Smartphone*, se sabem quais são os dados que disponibilizam às várias organizações de telecomunicações e também se tomam medidas para se proteger.

Duração da entrevista: O tempo da entrevista será, aproximadamente, de 45 minutos.

<u>Experimentação</u>	Bibliografia
No Restaurante, em conversas privadas:	Pergunta adaptada com base no estudo de (Anshari & Alas, 2015), de forma a conseguir responder ao objetivo desta investigação.
<p>1. Onde deixa o <i>Smartphone</i> quando está no Restaurante, em conversas privadas?</p>	
<p>2. Desliga o <i>Smartphone</i> quando está no Restaurante, em conversas privadas?</p>	
<p>3. Desliga a internet quando está no Restaurante, em conversas privadas?</p>	

No casa de banho:	Pergunta adaptada com base no estudo de (Anshari & Alas, 2015), de forma a conseguir responder ao objetivo desta investigação.
4. Onde deixa o <i>Smartphone</i> quando está na casa de banho?	
5. Desliga o <i>Smartphone</i> quando está na casa de banho?	
6. Desliga a internet quando está na casa de banho?	

Em momentos íntimos, como quando vai dormir:

Pergunta adaptada com base no estudo de (Anshari & Alas, 2015), de forma a conseguir responder ao objetivo desta investigação.

7. Onde deixa o *Smartphone* em momentos íntimos, como quando vai dormir?

8. Desliga o *Smartphone* em momentos íntimos, como quando vai dormir?

9. Desliga a internet em momentos íntimos, como quando vai dormir?

Em Casa:

Pergunta adaptada com base no estudo de (Anshari & Alas, 2015), de forma a conseguir responder ao objetivo desta investigação.

10. Onde deixa o *Smartphone* quando está na casa?

11. Desliga o *Smartphone* quando está na casa?

12. Desliga a internet quando está na casa?

Nas aulas ou no trabalho:	Pergunta adaptada com base no estudo de (Anshari & Alas, 2015), de forma a conseguir responder ao objetivo desta investigação.
13. Onde deixa o <i>Smartphone</i> quando está nas aulas ou no trabalho?	
14. Desliga o <i>Smartphone</i> quando está nas aulas ou no trabalho?	
15. Desliga a internet quando está nas aulas ou no trabalho?	
Nos transportes:	Pergunta adaptada com base no estudo de (Anshari & Alas, 2015), de forma a conseguir responder ao objetivo desta investigação.

16. Onde deixa o *Smartphone* quando anda de transportes públicos?

17. Desliga o *Smartphone* quando anda de transportes públicos?

18. Desliga a internet quando anda de transportes públicos?

Conclusões por pergunta da entrevista

1. Onde deixa o <i>Smartphone</i> quando está no Restaurante em conversas privadas?	Nesta questão chegou-se à conclusão que todos entrevistados deixam o <i>Smartphone</i> em cima da mesa e ou no bolso.
2. Desliga o <i>Smartphone</i> quando está no Restaurante em conversas privadas?	Nesta questão chegou-se à conclusão que todos os oito entrevistados deixam o <i>Smartphone</i> ligado.
3. Desliga a internet quando está no Restaurante em conversas privadas?	Nesta questão chegou-se à conclusão que três desligam a internet e cinco deixam a internet ligada. No entanto ninguém desliga a internet por causa de se preocupar com a sua privacidade. Os que desligam os dados móveis só o fazem para não gastar os dados móveis disponíveis do seu pacote.
4. Onde deixa o <i>Smartphone</i> quando está na casa de banho?	Nesta questão chegou-se à conclusão que todos levam o telemóvel para a casa de banho. Sendo que os oito entrevistados levam o <i>Smartphone</i> para a casa de banho em muitas ocasiões.
5. Desliga o <i>Smartphone</i> quando está na casa de banho?	Nesta questão chegou-se à conclusão que ninguém desliga o <i>Smartphone</i> quando vai á casa de banho. Os oito afirmam que deixam o <i>Smartphone</i> ligado.
6. Desliga a internet quando está na casa de banho?	Nesta questão chegou-se à conclusão que sete dos alunos não desligam a internet quando vão à casa de banho e apenas um desliga a internet quando vai à casa de banho. O aluno que desliga a internet na casa de banho diz que o faz porque se sente mais seguro. No entanto todos os entrevistados usam o <i>Smartphone</i> em certas ocasiões na casa de banho.
7. Onde deixa o <i>Smartphone</i> em momentos íntimos como quando vai dormir?	Nesta questão chegou-se à conclusão que todos levam o <i>Smartphone</i> para o quarto, sendo que dois deixam o <i>Smartphone</i> com eles até mesmo na cama.

8.	Desliga o <i>Smartphone</i> em momentos íntimos como quando vai dormir?
	Nesta questão chegou-se à conclusão que nenhum dos participantes desliga o <i>Smartphone</i> em momentos íntimos como quando vão dormir.
9.	Desliga a internet em momentos íntimos como quando vai dormir?
	Nesta questão chegou-se à conclusão que cinco dos alunos desligam a internet nos seus momentos íntimos como quando vão dormir e três deixam a internet ligada.
10.	Onde deixa o <i>Smartphone</i> quando está em casa?
	Nesta questão chegou-se à conclusão que quatro dos participantes andam com o <i>Smartphone</i> , dois dos participantes deixam o <i>Smartphone</i> ficar em qualquer lado e dois deixam o <i>Smartphone</i> em cima da mesa.
11.	Desliga o <i>Smartphone</i> quando está em casa?
	Nesta questão chegou-se à conclusão que sete dos inquiridos não desliga o <i>Smartphone</i> em casa e apenas um desliga o <i>Smartphone</i> em casa. Sendo que o entrevistado que desliga o <i>Smartphone</i> em casa apenas o liga quando precisa de o utilizar, mas também afirma que não o faz por motivos de segurança da sua privacidade. Todos utilizam o <i>Smartphone</i> em casa.
12.	Desliga a internet quando está em casa?
	Nesta questão chegou-se à conclusão que sete dos inquiridos não desliga a internet em casa e apenas um desliga a internet quando está em casa. Sendo que este indica não o fazer por motivos de segurança da sua privacidade.
13.	Onde deixa o <i>Smartphone</i> quando está nas aulas ou no trabalho?
	Nesta questão chegou-se à conclusão que quatro dos inquiridos deixa o <i>Smartphone</i> no bolso, três em cima da mesa e um deles deixa o <i>Smartphone</i> na bolsa.
14.	Desliga o <i>Smartphone</i> quando está nas aulas ou no trabalho?
	Nesta questão chegou-se à conclusão que nenhum dos oito participantes desliga o <i>Smartphone</i> nas aulas ou no trabalho.
15.	Desliga a internet quando está nas aulas ou no trabalho?

Nesta questão chegou-se à conclusão que sete dos alunos não desligam a internet e um desliga a internet durante as aulas ou no trabalho.

16. Onde deixa o *Smartphone* quando anda de transportes públicos?

Nesta questão chegou-se à conclusão que todos guardam o *Smartphone* quando não o estão a usar, cinco guardam este no bolso e três guardam este na sua bolsa.

17. Desliga o *Smartphone* quando anda de transportes públicos?

Nesta questão chegou-se à conclusão que nenhum dos participantes desliga o *Smartphone* quando anda em transportes públicos, três dizendo que tem de estar contactáveis.

18. Desliga a internet quando anda de transportes públicos?

Nesta questão chegou-se à conclusão que sete dos estudantes não desligam a internet e um desliga a internet nos transportes públicos. O inquirido que desliga a internet, afirma que a razão para desligar a internet nessas situações é para evitar gastar os dados móveis do seu pacote de dados.

Apêndice F – Métodos de análise descritiva

Métodos de análise descritiva usados neste trabalho

O primeiro é o teste Qui-quadrado de Independência, sendo p_{ij} a probabilidade de um indivíduo ser classificado nas categorias i ($i = 1, \dots, r$) e j ($j = 1, \dots, s$), (Hair Jr. et al., 2006), em que seja a probabilidade marginal de um indivíduo a ser classificado numa categoria i da variável X_i , e a probabilidade marginal de um indivíduo ser classificado na categoria j da variável Y_j .

$$p_{\cdot j} = \sum_{i=1}^r p_{ij}$$

Figura 17 – Equação

Fonte: (Hair Jr. et al., 2006)

A estatística de teste é dada pela seguinte equação da figura 18, onde χ^2 é o valor da estatística de teste qui-quadrado, O_{ij} é o valor observado na i -ésima e j -ésima posição e E_{ij} é o valor esperado na i -ésima e j -ésima posição.

$$\chi^2 = \sum_{i=1}^r \sum_{j=1}^s \frac{(O_{ij} - E_{ij})^2}{E_{ij}}$$

Figura 18 – Equação Qui-quadrado de independência

Fonte: (Hair Jr. et al., 2006)

Correlação de V de Crámer

O coeficiente *V de Crámer* é uma medida de associação entre duas variáveis, medidas numa escala categórica, sendo um tipo de teste não paramétrico. Deste modo, pode ser aplicado em situações onde a informação se encontre distribuída por categorias nominais não ordenáveis. Este coeficiente obtém-se diretamente a partir da estatística χ^2 , onde n representa o número total de observações e l representa o mínimo entre o número de linhas

e colunas da tabela de contingência. É utilizado para medir a intensidade da associação de variáveis nominais. O seu valor varia entre $0 \leq V \leq 1$, onde zero mostra a ausência de associação entre as duas variáveis e um mostra uma associação completa entre as duas variáveis (David J. Sheskin, 2004).

$$V = \sqrt{\frac{X^2}{n(l-1)}}$$

Figura 19 – Equação Correlação de V Crámer

Fonte: (Field, 2013)

Odds Ratio

A razão de chance ou *odds ratio*, de um modo geral, é definida como a razão entre a chance de um evento acontecer num grupo e a chance de ocorrer noutro grupo, sabendo que $E(Y_i) = \pi_i$. Esta chance é definida pela equação da figura 20.

$$RC = \frac{P(Y_i = 1 / X_i)}{P(Y_i = 0 / X_i)} = \frac{\pi_i}{1 - \pi_i}$$

Figura 20 – Equação Odds Ratio (Razão de chances)

Fonte: (Rudas, 2011)

Assim sendo, Rudas (2011) afirma que, quando $\pi_i = (1 - \pi_i)$ for um número superior ou inferior a 1, tem-se que o valor inteiro corresponde à chance das vezes a mais ou a menos (dependendo do sinal da estimativa dos parâmetros) que um determinado evento poderá ocorrer, em relação a outro sob as mesmas condições. Quando este valor for igual ou próximo ao valor 1, a razão de chance permanece constante, ou seja, tem-se a mesma chance de ocorrência dos eventos, sob as mesmas condições.

Apêndice G – Guião do questionário

Guião para questionários relacionado com o tema “A privacidade dos dados pessoais na era dos *Smartphones*”

Introdução sobre o tema: Olá, o meu nome é Bruno Oliveira. Muito obrigado por fazerem parte do meu estudo. Estou a fazer uma dissertação, aqui, no ISCTE-IUL sobre a privacidade dos dados pessoais, na era dos *Smartphones*, entre estudantes universitários.

Objetivo da questionário: O objetivo deste questionário é perceber se os estudantes universitários do primeiro ano da escola ISTA do ISCTE-IUL sabem que a sua privacidade pessoal está em risco, quando usam o *Smartphone*. Pretende-se também verificar se sabem quais os dados que disponibilizam às várias organizações de telecomunicações e se tomam medidas para se proteger.

Duração do questionário: O tempo necessário para responder a este questionário será, aproximadamente, de 20 minutos.

Consentimento Informado

Estamos a solicitar a sua participação num estudo sobre a privacidade de dados pessoais com *Smartphones*. Este estudo tem como objetivo perceber o que os estudantes pensam sobre a privacidade dos dados pessoais, no mundo digital, e quais os comportamentos que têm com *Smartphones*. Para este fim, solicitamos a sua participação num questionário, no qual vamos recolher os dados sobre a utilização deste telemóvel com certas aplicações e a ligação à internet.

Tudo o que partilhar neste questionário será estritamente confidencial. Os resultados serão anónimos. Gostaríamos de saber se aceita participar neste questionário.

O questionário é preenchido voluntariamente pelos estudantes.

Nº de Pergunta	Pergunta	Bibliografia / Nº Pergunta	Aplicação	Questões de investigação associadas
Grupo 1	Dados Sociodemográficos (DS)			
1	1. Género Feminino/Masculino	(Messias, 2017) / 1		
2	2. Data de Nascimento <1945, 1945-1964, 1965-1979, 1980-1990, 1991-2000, >2000	(Messias, 2017) / 2		
3	3. Indique a área do seu Curso: Arquitetura e Urbanismo, Engenharia de Telecomunicações e Informática, Engenharia Informática, Informática e gestão de empresas	(Cristina Hedler et al., n.d.) / DS3		
Grupo 2	Perfil tecnológico (PT)			
4	Maioritariamente, utiliza a Internet no seu <i>Smartphone</i> para: E-mail, notícias, televisão, Redes sociais, jogar, páginas web, pesquisa de conteúdos, aprender informalmente, participar em fóruns, trabalhar colaborativamente, estudar, ver videos, outros.	(Messias, 2017) / 8		d), g) 4)
5	Há quantos anos tem <i>Smartphone</i> pessoal? <1, 1-3, 4-6, 6-8, >8	Pergunta adaptada do estudo de Messias (2017) 7.4.1, de forma a conseguir responder ao objetivo desta investigação.		i) 4)
6	Indique como se liga à Internet com o <i>Smartphone</i> : Rede Wi-Fi privada de casa, Rede Wi-Fi de amigos, Rede Wi-Fi de trabalho, Rede móvel privada da sua operadora, Redes Wi-Fi publicas em lugares públicos, Redes Wi-Fi	(Delac et al., 2011) (Xiong & Jamieson, 2013)		d) 4)

	desconhecidas que oferecem Internet gratuita			
7	Indique quais destas aplicações usa no seu <i>Smartphone</i> : câmara, GPS, navegador Web, calendário, e-mail, agenda de contactos, mensagens, chamadas	(Messias, 2017) / 17		d) 1), 4)
8	Com que frequência está online na sua aplicação preferida? Estou sempre ligado, Várias vezes por dia, 3 a 4 vezes por dia, Uma vez por semana, Ocasionalmente (menos do que uma vez por semana)	(Messias, 2017) / 21		h), i), d) 4)
9	Ao aderir a uma rede ou quando compra equipamento tem o hábito de: Ler as instruções ou ler sobre de que se trata, Abrir usar imediatamente aprendendo por tentativa de erro, Abrir/Entrar e usar imediatamente, mas, sempre que necessário, consultar o manual ou instruções	(Messias, 2017) / 13		i) 4)
10	Indique qual a informação que inclui no seu perfil da conta do seu <i>Smartphone</i> ? Outros, Estado Civil, Nome real, Orientação política, Fotos pessoais, Fotos de outros, Número de telemóvel/telefone, Endereço de IM (Instant Messege), Local de residência, Naturalidade (cidade), Endereço de email	(Messias, 2017) / 23		e), f) 1), 2), 4)
12	Aceita os termos de aceitação quando estas implicam ter acesso aos dados de posicionamento do seu <i>Smartphone</i> ? Sim/Não	Pergunta adaptada com base no estudo de Obar & Oeldorf-Hirsch (2018), de forma a conseguir responder ao objetivo desta investigação.		e), f) 1), 2)

13	Na sua opinião, até que ponto sente que o <i>Smartphone</i> afeta os seus estudos? Afetam bastante de forma positiva, Afetam bastante de forma negativa, Não tem qualquer impacto, Afetam ligeiramente de forma positiva, Afetam ligeiramente de forma negativa	(Messias, 2017) / 35		g), i) 4)
ALT Grupo 3	Teoria do Nível de Adaptação	(Expectativas iniciais dos utilizadores individuais são a base de comparação do seu nível de adaptação.) (O nível de adaptação é a comparação entre a expectativa inicial, e o desempenho real percebido.)		
14	Numa escala de 1 a 5, previamente a ter um <i>Smartphone</i> , considerava que a utilização das aplicações de comunicação do <i>Smartphone</i> teriam riscos para a sua privacidade? 1- Nenhum risco, 2-Poucos riscos, 3-Risco neutro, 4-Bastantes riscos, 5-Muitos riscos	Pergunta adaptada com base no estudo de Vallina-Rodriguez & Sundaresan (2017), de forma a conseguir responder ao objetivo desta investigação.		a), b), f) 2
15	Numa escala de 1 a 5, previamente a ter um <i>Smartphone</i> , considerava que poderia confiar a partilha de informação inerente à utilização das aplicações necessárias ao funcionamento deste dispositivo? 1- Não Confiava, 2- Confiava pouco, 3- Opinião neutra, 4- Confiava Bastante, 5- Confiava Muito	Pergunta adaptada com base no estudo de Dwyer, Roxanne Hiltz, Passerini, & Roxanne, 2007; Shin (2010), de forma a conseguir responder ao objetivo desta investigação.		a), b), c), e) 1, 2

16	<p>Numa escala de 1 a 5, previamente a ter um <i>Smartphone</i>, considerava que a utilização do mesmo iria ter riscos de privacidade relativamente aos dados móveis que iria partilhar?</p> <p>1-Nenhuns riscos, 2-Poucos riscos, 3-Risco neutro, 4-Alguns riscos, 5-Muitos riscos</p>	<p>Pergunta adaptada com base no estudo de Lell & Nohl (2018), de forma a conseguir responder ao objetivo desta investigação.</p>		<p>a), b), c), e) 1, 2</p>
17	<p>Numa escala de 1 a 5, previamente a ter um <i>Smartphone</i>, considerava que a utilização da câmara do <i>Smartphone</i> iria ter riscos de segurança?</p> <p>1- Nenhum riscos, 2- Poucos riscos, 3- Risco neutro, 4- Alguns riscos, 5- Muitos riscos</p>	<p>Pergunta adaptada com base no estudo de Deshpande & Dharmadhikari (2016), de forma a conseguir responder ao objetivo desta investigação.</p>		<p>a), b), c), e), f) 1, 2</p>
18	<p>Numa escala de 1 a 5, previamente a ter um <i>Smartphone</i>, considerava que seria necessário instalar uma aplicação para manter o seu direito à privacidade aquando a utilização deste dispositivo? 1-Nada necessário, 2-Pouco necessário, 3- Necessidade neutra, 4-Bastante necessário, 5-Muito necessário</p>	<p>Pergunta adaptada com base nos estudos de Warren & Brandeis (1890) e (Delac et al., 2011), de forma a conseguir responder ao objetivo desta investigação.</p>		<p>a), b), c), e), f) 1, 2</p>
TDC Grupo 4	Teoria da Dissonância Cognitiva	(Usar escalas de Likert de 1 – 5)		
19	Houve alturas em que me preocupei com a minha privacidade ao utilizar o <i>Smartphone</i> . Sim/Não	(Levin et al., 2013) / 2	Todas	a), e), b), f) 2), 3), 4), 5)
20	Concorda em não comprar um <i>Smartphone</i> se pudesse voltar atrás? Sim/Não	(Levin et al., 2013) / 3		a) 3), 5)
21	Algumas funcionalidades do <i>Smartphone</i> não são consistentes com as minhas expetativas antes da utilização. Sim/Não	(Levin et al., 2013) / 4		a), g), i) 5

22	Sempre tive a certeza de como era a utilização do <i>Smartphone</i> . Sim/Não	(Levin et al., 2013) / 5		f), i), g) 5
23	Confio no meu <i>Smartphone</i> . Sim/Não	(Levin et al., 2013) / Q2		a), b), f) 2), 3), 4)
24	Sento-me confortável ao usar o <i>Smartphone</i> . Sim/Não	(Levin et al., 2013) / Q3		a), b), f) 2), 3), 4)
25	Utilizo bem o <i>Smartphone</i> . Sim/Não	(Levin et al., 2013) / Q5		a), b), i) 4
26	Ao ter conhecimento dos riscos de segurança, vou parar de usar o <i>Smartphone</i> . Sim/Não	(Levin et al., 2013) / Pergunta desenvolvida no meu estudo		e), f) 2), 3), 5)
Grupo 5	Uso do <i>Smartphone</i>			
27	Utiliza o <i>Smartphone</i> para uso académico? Sim/Não	Pergunta adaptada do estudo de Messias (2017) / 35, de forma a conseguir responder ao objetivo desta investigação. (Para identificar as redes que são utilizadas)		g), i) 4)
28	Com que regularidade, em média, utiliza o <i>Smartphone</i> ? Todos os dias, 4 a 6 dias por semana, 2 a 3 dias por semana, 1 dia por semana, 2 dias por mês, 1 dia por mês	(Ferreira, 2014) / 1.1		h), i) 4
29	Em média, quanto tempo gasta, por dia, no <i>Smartphone</i> ? Menos de 1 hora, Entre 1 e 2 horas, Mais de 3 horas	(Ferreira, 2014) / 1.2		h), i) 4
30	Há quanto tempo possui um <i>Smartphone</i> ? Há menos de 1 ano, Entre 1 a 3 anos, Há mais de 3 anos	(Ferreira, 2014) / 1.3		i) 4
31	Em média, quantas horas por semana utiliza o <i>Smartphone</i> ? <6h, 6h-10h, 11h-20h, 21h-30h, 31h-40h, 41h-50h, >50h	(Messias, 2017) / 20		h), i) 4

TAM Grupo 6	Facilidade de uso percebida (FUP)			
32	Numa escala de 1 a 5, considera que é fácil aprender a utilizar o <i>Smartphone</i> ? 1-Nada fácil, 2-Pouco fácil, 3-Facilidade neutra, 4-Bastante fácil, 5-Muito fácil	(Ferreira, 2014) / 3.1		i) 4
33	Numa escala de 1 a 5, considera que a utilização do <i>Smartphone</i> não requer muito esforço mental? 1-Nenhum esforço, 2-Pouco esforço, 3-Esforço neutro. 4-Algum esforço, 5-Muito esforço	(Ferreira, 2014) / 3.2		i) 4
34	Numa escala de 1 a 5, considera fácil comunicar com os seus contatos através do <i>Smartphone</i> ? 1-Nada fácil, 2-Pouco fácil, 3-Facilidade neutra, 4-Bastante fácil, 5-Muito fácil	(Ferreira, 2014) / 3.4		g), i) 4
35	As ferramentas do <i>Smartphone</i> são flexíveis para que eu possa usá-las da maneira que melhor me convier. Sim/Não	(Cristina Hedler et al., n.d.) 7 FUP4		g), i) 4
36	Numa escala de 1 a 5, considera fácil partilhar fotos/vídeos / estados no <i>Smartphone</i> ? 1-Nada fácil, 2-Pouco fácil, 3-Facilidade neutra, 4-Bastante fácil, 5-Muito fácil	(Ferreira, 2014) / 3.3		g), i) 4
37	Numa escala de 1 a 5, considera a interação com o <i>Smartphone</i> como flexível? (relativamente ao leque de aplicações disponíveis) 1-Nada flexível, 2-Pouco flexível, 3- Flexibilidade neutra, 4-Bastante flexível, 5-Muito flexível	(Gao, Krogstie, & Siau, 2011) / EOU 4		g), i) 4
TAM Grupo 7	Utilidade percebida (UP)			

38	Numa escala de 1 a 5, considera o <i>Smartphone</i> útil para comunicar com a sua rede de contactos pessoais (amigos)? 1-Nada útil, 2-Pouco útil, 3-Utilidade neutra, 4-Bastante útil, 5-Muito útil	(Ferreira, 2014) / 2.2	Mensagens Microfone Email Contactos	g), i) 4)
39	Numa escala de 1 a 5, considera o <i>Smartphone</i> útil para comunicar com a sua rede de contactos universitários? 1-Nada útil, 2-Pouco útil, 3-Utilidade neutra, 4-Bastante útil, 5-Muito útil	(Ferreira, 2014) / 2.3	Mensagens Microfone Email Contactos	g), i) 4)
40	Numa escala de 1 a 5, considera útil ter a possibilidade de partilhar fotos/vídeos /ficheiros pelo <i>Smartphone</i> ? 1-Nada útil, 2-Pouco útil, 3-Utilidade neutra, 4-Bastante útil, 5-Muito útil	(Ferreira, 2014) / 2.5	todas	g), e), i) 4)
41	Ao usar ferramentas do <i>Smartphone</i> o meu trabalho fica mais rápido? Sim/Não	(Cristina Hedler et al., n.d.) / UP1	todas	g), h), i) 4)
42	Usar o <i>Smartphone</i> aumenta a eficiência no trabalho do meu dia a dia? Sim/Não	(Gao et al., 2011) / PU 1	todas	g), h), i) 4)
43	Numa escala de 1 a 5, indique até que ponto sente que o <i>Smartphone</i> afeta os seus estudos: 1-Não afeta nada, 2-Afeta pouco, 3-Não tem qualquer impacto, 4-Afeta bastante, 5-Afeta muito	(Messias, 2017) / 35	todas	g), h), i) 4)
44	Numa escala de 1 a 5, previamente a ter um <i>Smartphone</i> , considerava que a utilização do <i>Smartphone</i> iria ser útil nos seus estudos? 1-Nada útil, 2-Pouco útil, 3-Utilidade neutra, 4-Bastante útil, 5-Muito útil	Pergunta adaptada do estudo de Messias (2017) / 35, de forma a conseguir responder ao objetivo desta investigação. (Para identificar as redes que são utilizadas)		g), h), i) 4)
TAM Grupo 8	Intenção Comportamental (IC)			

45	Quero utilizar o <i>Smartphone</i> , sempre que possível. Sim/Não	(Cristina Hedler et al., n.d.) / IC1	todas	g), h) i) 4), 5)
46	Tenho a intenção de aumentar o uso das ferramentas no <i>Smartphone</i> . Sim/Não	(Cristina Hedler et al., n.d.) / IC2	todas	g), b), h), i) 3, 4, 5
47	Adorava ter novas ferramentas no meu <i>Smartphone</i> , no futuro. Sim/Não	(Cristina Hedler et al., n.d.) / IC3		b), d), h), i) 4, 3
48	Tenho necessidade de tapar a câmara do <i>Smartphone</i> em algumas situações. Sim/Não	Pergunta adaptada do estudo de Deshpande & Dharmadhikari (2016), de forma a conseguir responder ao objetivo desta investigação.	Câmera	a), b), c), d), f), i) 1, 2, 3, 4, 5
49	Tenho necessidade de desligar o GPS sempre que não precisa? Sim/Não	Pergunta adaptada do estudo de Wang & Loui (2009), de forma a conseguir responder ao objetivo desta investigação.	GPS	a), b), c), d), f), i) 1,2,3,4,5
50	Sinto necessidade de desligar o <i>Smartphone</i> por completo durante os períodos em que não o estou a usar, por questões de segurança? Sim/Não	Pergunta adaptada com base nos estudos de Warren & Brandeis (1890), (Delac et al., 2011) e (Xiong & Jamieson, 2013), de forma a conseguir responder ao objetivo desta investigação.	Todas	a), b), c), d), f) 1,2,3,4,5
51	Tenho intenção de adquirir uma aplicação para me defender da invasão de terceiros? (antivírus) Sim/Não	Pergunta adaptada com base nos estudos de Warren & Brandeis (1890), (Delac et al., 2011) e (Xiong & Jamieson, 2013), de forma a conseguir responder ao objetivo desta investigação.		a), b), c), d), f) 1,2,3,4,5

52	Adorava ter um botão que me permitisse ligar e desligar o microfone do meu <i>Smartphone</i> . Sim/Não	Pergunta adaptada com base no estudo de Waheed & Khan (2010), de forma a conseguir responder ao objetivo desta investigação.	Microfone	a), b), c), d), f) 1,2,3,4,5
TAM Grupo 9	Uso real (UR)			
53	Indique quais destas aplicações usa frequentemente no seu <i>Smartphone</i> ? Páginas Web, GPS, Calendário, E-mail, Contactos, Camaras, Microfone, Mensagens	(Messias, 2017)	Todas	d), f) 1), 4)
54	Com que frequência usa ferramentas do <i>Smartphone</i> ? 1-Todos os dias, 2-Duas vezes por semana, 3-Três vezes por semana, 4-Quatro vezes por semana, 5-Cinco ou seis vezes por semana	(Cristina Hedler et al., n.d.) / UR2	Todas	h), d) 1,4
55	Costumo usar o meu <i>Smartphone</i> para partilhar dados/fotografias. Sim/Não	Pergunta adaptada com base no estudo de Meng et al. (2018), de forma a conseguir responder ao objetivo desta investigação.	Todas	e), g) 1), 4)
56	Costuma usar o <i>Smartphone</i> para monitorizar a sua atividade física/desportiva? Sim/ Não	Pergunta adaptada com base no estudo de Meng et al. (2018), de forma a conseguir responder ao objetivo desta investigação.		e), g), i) 1), 4)
57	Costuma usar o GPS do seu <i>Smartphone</i> para atividades físicas? Sim/Não	Pergunta adaptada com base no estudo de Wang & Loui (2009), de forma a conseguir responder ao objetivo desta investigação.	GPS	e), g), i), d) 1), 4)
TAM Grupo 10	Confiança/Segurança			

58	Divulga as suas informações pessoais no <i>Smartphone</i> ? Sim/Não	(Ferreira, 2014) / 7.1	Todas	e), a), b), f), c) i) 1), 2), 4), 5)
59	Numa escala de 1 a 5, considera o <i>Smartphone</i> um meio seguro para partilhar fotos/ vídeos/ ficheiros/ informações pessoais? 1- Nada seguro, 2-Pouco seguro, 3-Segurança neutra, 4-Bastante seguro, 5-Muito seguro	(Ferreira, 2014) / 7.3	Todas	e), a), b), f), c) i) 1), 2), 4), 5)
60	No geral, e numa escala de 1 a 5, sente-se plenamente seguro em utilizar o <i>Smartphone</i> , para comunicar com os seus contactos ou empresas? 1- Nada seguro, 2-Pouco seguro, 3-Segurança neutra, 4-Bastante seguro, 5-Muito seguro	(Ferreira, 2014) / 7.5	Todas	e), a), b), c), f), i) 1), 2), 4), 5)
61	No geral, e numa escala de 1 a 5, sente-se plenamente seguro em utilizar o <i>Smartphone</i> para jogar as mais diversas aplicações disponibilizadas no <i>Smartphone</i> ? 1-Nada seguro, 2-Pouco seguro, 3-Segurança neutra, 4-Bastante seguro, 5-Muito seguro	Pergunta adaptada com base no estudo de Meng et al. (2018), de forma a conseguir responder ao objetivo desta investigação.	Todas	e), a), b), c), f), i) 1), 2), 4), 5)
62	Sente-se seguro a utilizar o <i>Smartphone</i> para ter conversas privadas, relacionadas com o trabalho ou dados sensíveis? 1-Nada seguro, 2-Pouco seguro, 3-Segurança neutra, 4-Bastante seguro, 5-Muito seguro	Pergunta adaptada com base no estudo de Waheed & Khan (2010), de forma a conseguir responder ao objetivo desta investigação.	Micro fone	e), a), b), c), f), i) 1), 2), 4), 5)

Perguntas TAM – Amarelo
Perguntas TDC – Verde
Perguntas ALT – Roxo

Objetivos de investigação a responder neste estudo

- a) Determinar o nível de confiança desta população com as organizações;
- b) Determinar se a população em estudo se sente segura, relativamente à sua privacidade pessoal, ao usar o *Smartphone* e as suas aplicações;
- c) Determinar o nível de satisfação do tratamento dos dados privados da população pelas organizações;
- d) Determinar o comportamento com o *Smartphone* ligado à internet, GPS, câmara, microfone;
- e) Determinar se a população estudada sabe que tipo de informações está a disponibilizar aos vários tipos de organizações;
- f) Determinar se a população em estudo aceita que as organizações tenham acesso a todos os dados privados introduzidos no *Smartphone*;
- g) Determinar se o *Smartphone* traz vantagens no dia-a-dia para o utilizador.
- h) Determinar a quantidade de utilização *Smartphone*;
- i) Determinar se o utilizador é *digitally savvy*;
- 1) Determinar o tipo de informações que os utilizadores estão a fornecer às organizações que disponibilizam os serviços, através dos *Smartphones*;
- 2) Determinar se a população estudada sabe que tipo de informações está a disponibilizar a terceiros, ao usar o seu telemóvel;
- 3) Compreender e identificar se é preciso tomar medidas futuras, de forma a proteger a privacidade digital de cada utilizador, para garantir uma utilização dos *Smartphones* que deixe os utilizadores sem medo de expor a sua privacidade;
- 4) Perceber que utilização as pessoas fazem dos seus dispositivos móveis;
- 5) Determinar se a população aceita ter uma vida digital transparente no futuro.