Instituto Universitário de Lisboa

Departamento de Ciências e Tecnologias da Informação

Está por aí alguém?
Perceções da exposição e da privacidade nas redes sociais, entre estudantes universitários

Nelson Jorge dos Santos Rodrigues

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Gestão de Sistemas de Informação

Orientador(a):
Doutor Abílio Gaspar de Oliveira, Professor Auxiliar,
ISCTE-IUL

outubro, 2018

“If you want to keep a secret, you must also hide it from yourself.”

George Orwell, Nineteen Eighty-Four, 1949

Agradecimentos

Este projeto sendo individual foi na realidade fruto de um esforço coletivo, apenas possível graças à colaboração, apoio, tolerância e dedicação de todos aqueles que nele, de uma forma ou outra intervieram, aos quais quero aqui deixar o meu profundo agradecimento.

Ao meu filho, esposa, mãe, pai, irmão e a toda a restante família pelo apoio, carinho, presença, disponibilidade e compreensão que me dedicaram ao longo destes dois anos pelas horas investidas no mestrado de uma forma geral e nesta dissertação em particular.

Ao Professor Abílio Oliveira, pela sua orientação, motivação, clarividência e por ter sempre acreditado em mim. Obrigado acima de tudo por muitas palavras proferidas nos momentos de maior necessidade.

Ao Professor Bráulio Alturas e à Professora Inês Messias pela disponibilidade e pelo contributo com que granjearam este trabalho.

Aos meus colegas de mestrado, em particular o Jorge, a Catarina e a Andreia pelo companheirismo e palavras de incentivo nos momentos mais extenuantes.

A todos aqueles que despenderam um pouco do seu tempo para contribuir para este estudo, em especial às alunas Ana Filipa Rodrigues e Sara Bonifácio pela inestimável ajuda em tornar possível a execução do *focus group*.

A todos, os meus profundos agradecimentos, obrigado.

Resumo

As redes sociais online têm conhecido uma taxa de adoção mundial sem precedentes no universo das tecnologias de informação. Não obstante as inúmeras vantagens decorrentes da utilização das redes sociais online, estes sistemas vivem da partilha de informação, por vezes privada, dos seus utilizadores. Apesar das redes sociais oferecerem inúmeras funcionalidades de gestão de definições e preferências de privacidade e segurança, muitos utilizadores optam – de forma consciente ou não – em efetuar uma partilha excessiva, ou não controlada, de informação pessoal com as redes sociais. A partilha controlada (ou não!) de informação pessoal nas redes sociais pode colocar as pessoas em situações de risco ou até mesmo de ameaça, quer ao próprio individuo quer a outras pessoas da sua rede de contactos ou família.

Este projeto visa, sobretudo, compreender como é que os estudantes universitários percecionam o modo como se expõem online e a importância que isso tem na sua privacidade e na segurança da informação partilhada nas redes sociais. Foram desenvolvidos dois estudos, um exploratório e outro inferencial. No primeiro, mais qualitativo, foram realizadas entrevistas com especialistas e um *focus group* com estudantes universitários, daí resultando indicadores usados posteriormente, na elaboração de um questionário, no segundo estudo, de índole mais quantitativa. Entre os principais resultados, constatou-se uma elevada preocupação dos estudantes com a sua privacidade nas redes sociais, porém, mais na teoria do que na prática, havendo, assim discrepâncias entre as suas perceções (ou opiniões) e os seus comportamentos (ou atitudes) típicos, nas redes sociais. Pelo que, este trabalho permite contribuir para avaliar a distorção entre as perceções que os estudantes têm da sua exposição online, da salvaguarda da sua privacidade, e os reais comportamentos que exibem no uso diário das redes sociais.

Palavras-Chave: Redes Sociais, Segurança de Informação, Privacidade online, Perceção de Segurança, Perceção de Privacidade, Confiança nas Redes Sociais e Controlo da Informação.

Abstract

Social Network Services have seen an unprecedented adoption rate in the world of information technology. Notwithstanding the numerous benefits of using social networking services, these systems live from the sharing of information, sometimes private, from their users. Although social network services have numerous privacy and security settings and management features, many users choose - consciously or unintentionally - to make excessive or uncontrolled sharing of personal information with social network services. This controlled sharing (or not!) of personal information on social networks can put people at risk or even threatening situations, either to the individual himself or to others in his network or family.

This project aims to understand how university students perceive the way they expose themselves online and the importance that this has on their privacy and the security of information shared in social networks. Two studies were developed, one exploratory and another inferential. On the first, more qualitative, were conducted interviews with specialists and a focus group with college students, resulting in indicators used later to produce a questionnaire carried out on the second study, of a more quantitative nature. Among the main results, there was a high concern on students for their privacy in social networks, but more in theory than in practice. So, there are discrepancies between their perceptions (or opinions) and their typical behaviours (or attitudes), in social networks. Therefore, this work contributes to evaluate the distortion between students' perceptions of their online exposure, the safeguarding of their privacy, and the real behaviours they exhibit in the daily use of social networks.

Keywords: Social Network Services, Information Security, Online privacy, Perceived Security, Perceived Privacy, Trust in Social Networks and Information Control.

Índice

Índice de Tabelas

Índice de Figuras

Lista de Abreviaturas e Siglas

ACP – Análise de Componentes Principais

BFAS – The Bergen Facebook Addiction Scale

IoT – Internet of Things

OSN – Online Social Networks

PbD – Privacy by Design

RGPD – Regulamento Geral de Proteção de Dados

RSS – Really Simple Syndication, Rich Site Summary

SMS – Short Message Text

SNS – Social Networking Services

SPSS – Statistical Package for the Social Sciences

TIC – Tecnologias de Informação e Comunicação

TRA – Theory Reasoned Action

UE – União Europeia

VPN – Virtual Private Network

Capítulo 1 – Introdução Geral

1.1. Enquadramento do tema

Desde o seu aparecimento os sites de redes sociais, tais como o Facebook, o Twitter, o LinkedIn, o Pinterest, ou o Instagram têm atraído milhões de utilizadores. Para muitas das pessoas que usam as redes sociais, o uso destas plataformas passou a fazer parte das suas rotinas diárias. Com a massificação das tecnologias móveis, tem-se verificado uma crescente ubiquidade das redes sociais no quotidiano das pessoas. Esta omnipresença é de tal forma intensa, que em alguns casos podem mesmo desenvolver-se patologias verdadeiramente obsessivas (Andreassen, *et.al.*, 2012; Stieger, *et.al.*, 2013).

Bem desde o início da massificação da Internet (1995) que se sabe que a exposição intensiva à *world wide web* provoca o declínio da comunicação familiar, a redução do círculo social e um aumento da depressão e solidão dos indivíduos (Castells, 2002). É exatamente esta contração do círculo social que impele o uso das redes sociais por forma a compensar o défice social. Os sites de redes sociais são excelentes meios para o desenvolvimento de múltiplos laços fracos, por sua vez estes laços fracos são ótimos veículos para a obtenção de informação e de oportunidades (Castells, 2002).

Um site de rede social trata-se de um serviço baseado na Internet que permite às pessoas construir perfis públicos ou semipúblicos, criar listas de outros utilizadores com quem partilham uma conexão, ver e cruzar as suas listas de conexões com as dos outros utilizadores, todas estas iterações ocorrem dentro de um sistema limitado (Boyd & Ellison, 2007, p. 211). Os sites de rede social são o pináculo da "privatização da sociabilidade" (Castells, 2002), isto é, agilizam a reconstrução do círculo social através de uma comunidade centrada no individuo, como que uma espécie de geocentrismo social.

Após a criação do primeiro site de rede social em 1997, o "SixDegrees.com", que se constatou uma grande apetência das pessoas por este tipo de tecnologia, isto induziu o aparecimento de centenas de sites de redes sociais, que em alguns casos cresceram de forma tão rápida que atraíram a atenção quer dos média quer da academia (Acquisti & Gross, 2006; Boyd & Ellison, 2007).

Apesar das redes sociais ofereceram todo um conjunto de oportunidades de interação entre os seus utilizadores, também atraem a atenção de não-utilizadores particularmente por questões relacionadas com a privacidade e a segurança. Estas preocupações podem

efetivamente estar fundamentadas, contudo os sites de redes sociais há muito que deixaram de ser fenómenos de nicho (Gross & Acquisti, 2005), milhões de pessoas em todo o mundo, de forma consciente e voluntária usam estas redes sociais para comunicar, encontrar amigos, marcar encontros e procurar empregos. Ao fazerem todas estas atividades, revelam deliberadamente informação pessoal não só a conhecidos como também a estranhos - por exemplo - datas de nascimento, números de telemóvel ou a morada atual são dados comuns nas redes sociais (Fogel & Nehmad, 2009; Kizza, 2001).

Não podemos deixar de nos maravilhar com a natureza, quantidade e detalhe de informação pessoal que alguns utilizadores providenciam, ao mesmo tempo devemos ponderar quão informada é esta partilha de informação (Gross & Acquisti, 2005). Existe uma baixa consciencialização dos utilizadores sobre como proteger a sua informação pessoal nas redes sociais (Nagy & Pecho, 2009) e nem sempre têm uma ideia clara sobre quem tem acesso a ela ou como esta poderá ser usada (Krishnamurthy & Wills, 2008).

Mais de 40% dos utilizadores de redes sociais partilham informação privada (Hajli & Lin, 2016), esta informação pode ser partilhada e usada sem o expresso consentimento do proprietário, colocando os utilizadores vulneráveis a vários perigos on-line tais como: fraude, roubo de identidade, *phishing*, entre outros. Assim que uma informação é colocada numa rede social esta deixa de ser efetivamente privada (Sadeghian, Zamani, & Shanmugam, 2013).

Tendo já registado taxas de crescimento na casa dos 3% por semana (Bilge, *et.al.*, 2009) e sendo o maior repositório de fotos na Internet o Facebook é sem dúvida a rede social *de facto*, esta hegemonia do Facebook aumenta também a sua atratividade para os criminosos, tendo surgido diversas peças de *software* capazes de lançar ataques automatizados que permitem o roubo de identidade ou a clonagem de perfis (Bilge, *et.al.*, 2009).

Além de informação pessoal, as redes sociais também permitem a partilha de conteúdo, conhecimento e experiências. Esta informação também ela pessoalmente identificável, pode rapidamente alimentar o desenho de perfis ou servir como massa crítica para fins comerciais sem o conhecimento dos utilizadores.

O uso de informação pessoal nas redes sociais levanta preocupações com a privacidade e segurança dos utilizadores, tendo surgido nos últimos anos como uma área de pesquisa de grande alcance e amplitude, variadíssimos estudos e notícias têm destacado o risco

acrescido para o processamento de dados pessoais por aplicações de redes sociais, assim como a falta de consciência da população em geral, deparamo-nos com um novo paradigma de segurança de informação (Ahn, *et.al.*, 2011).

Dispor de um perfil privado e devidamente seguro parece uma boa ideia para os utilizadores mais conscienciosos, contudo as suas ligações com outras pessoas e afiliações com grupos públicos também podem representar uma ameaça à sua segurança, pois é possível explorar as redes sociais de forma a prever informação pessoal e sensível dos utilizadores baseada em informação pública de grupos (Zheleva & Getoor, 2009).

Simultaneamente ao crescimento imbatível dos sites de redes sociais e das crescentes preocupações com a segurança decorrentes do seu uso, temos a adicionar ao *mix* os dispositivos móveis, que possuindo novas tecnologias vêm criar problemas acrescidos de segurança e privacidade ao coletar e disponibilizar informação privada dos utilizadores nas redes sociais, em concreto a localização geográfica (Kizza, 2001).

Para a maioria dos utilizadores os seus índices de preocupação relativamente à privacidade e segurança de um site de rede social estão relacionados com o controlo percecionado e a facilidade de acesso à informação, isto é, os utilizadores valorizam a existência de interfaces "*user-friendly*" que permitam definir as suas preferências de privacidade, aliviando assim as suas preocupações com a privacidade e segurança do sistema (Hoadley, *et.al.*, 2010).

Segundo Shin (2010, p. 430) a atitude dos utilizadores para com as redes sociais assenta sobre três pilares:

- Segurança: Perceção do utilizador sobre segurança, definida pela extensão em que um utilizador acredita que usar um sistema é livre de risco.
- Privacidade: Controlo do fluxo da informação pessoal, incluindo a transferência e troca dessa informação.
- Confiança: Confiança na rede social é definida como a disposição do utilizador em ficar vulnerável às ações do sistema de rede social, com base na expetativa que o sistema de rede social irá realizar uma ação particular importante para o utilizador, independentemente da capacidade do utilizador em monitorizar o sistema de rede social.

1.2. Motivação e relevância do tema

A escolha desta temática não poderia ser mais atual e desafiadora. Recentemente foi aprovada uma lei, nos Estados Unidos da América, que indica que os serviços de migração daquele país poderão requerer dados das redes sociais para a atribuição de vistos. Onde, diariamente nos meios de comunicação, se constata cada vez mais o aumento do "*cyberbullying*", com especial incidência nas redes sociais, afetando não só adolescentes como também adultos.

Por fim, a eminente entrada em vigor do Regulamento Geral de Proteção de Dados (RGPD) no espaço comunitário que vem, de forma coerciva, impor uma abordagem aos sistemas de informação das organizações focada no principio "*Privacy by design*", com uma aproximação proactiva ao invés de reativa (Cavoukian, 2011), que tem como primordial objetivo, lá está, salvaguardar a privacidade do indivíduo.

Em que medida as redes sociais vão conseguir proceder a adaptações que permitam, por um lado cumprir o RGPD, e por outro, conseguir manter os seus objetivos primordiais, que são, em última instância facilitar a partilha exaustiva e constante de dados potencialmente privados com sistemas de informação que não oferecem condições controlo sobre os dados e sua retenção.

É cada vez mais premente difundir e sensibilizar a comunidade em geral e a academia em particular, para os potenciais perigos da invasão das redes sociais na esfera da vida privada de cada cidadão perpetrada pelo próprio.

1.3. Implicações desta investigação

A principal implicação deste estudo prende-se com a explicação do comportamento online das pessoas relativamente à salvaguarda da sua esfera de privacidade e segurança. Os resultados do estudo irão aumentar o nível de alerta e de informação à disposição dos utilizadores, das organizações e dos legisladores, contribuindo assim para o alargamento das bases teóricas e factuais para a criação de regulamentação que promova a defesa dos interesses da informação de cada individuo, tendo como principal objetivo a redução dos riscos e ameaças a que os cidadãos, de uma forma geral, se expõem ao usaram as redes sociais online de forma não informada do potencial das mesmas. As vantagens desta regulamentação são diversas para o tecido da sociedade, temos o ponto de vista de segurança pública, o ponto de vista de saúde pública e acima de tudo a salvaguarda das

gerações mais novas, que estão gradualmente a perder as experiências de sociabilização e construção do individuo que caraterizaram as gerações pré-Internet e que providenciaram as ferramentas sociais para a criação de mecanismos naturais de defesa e autopreservação.

Esta melhor compreensão dos comportamentos nas redes sociais online relativamente à salvaguarda da privacidade vai também agilizar a massificação dos dispositivos "*wearable*" e das inúmeras aplicações IoT, permitindo às empresas responsáveis pelas plataformas de redes sociais online desenvolver políticas e ferramentas que ajudem a educar e alertar os utilizadores para o valor da sua informação e o seu uso. Produzindo eventualmente painéis de controlo em tempo real que mostrem o índice de privacidade, um mecanismo semelhante ao atual rating de força das passwords.

As empresas podem desenvolver procedimentos de recursos humanos que permitam avaliar os seus colaboradores sobre o risco e comportamentos de divulgação e conseguir aferir requisitos de nível de classificação proporcionais às suas posições (Hallam & Zanella, 2017).

O aparecimento de novas tecnologias, para além de todas as vantagens, acarreta também novos desafios éticos (Hajli & Lin, 2016), este documento explora algumas problemáticas do foro ético relativamente aos comportamentos dos utilizadores nas redes sociais online.

Por fim este estudo poderá auxiliar os fornecedores de redes sociais online a providenciar mais e melhor informação aos seus utilizadores de forma a reduzir a exposição e assim conseguir melhores rácios de compromisso entre os utilizadores e as plataformas de redes sociais online numa base de confiança e efetivo – em oposição do atual aparente – controlo dos dados.

1.4. Questões e objetivos de investigação

Este trabalho visa identificar e analisar em que medida os estudantes universitários têm perceção do impacto, ou importância, que a sua exposição online – em termos dos seus comportamentos, partilha de opiniões, conhecimentos e experiências –, em particular nas redes sociais, tem na sua esfera de privacidade. Ou seja, pretende-se percecionar as representações que estes têm acerca das redes sociais, do modo como se apresentam e

comunicam através das mesmas e da importância destas no seu quotidiano – em particular a nível pessoal.

A quantidade e detalhe de informação pessoal e familiar que alguns utilizadores providenciam nas redes sociais é avassaladora, ao mesmo tempo que a perceção que estes têm acerca dos impactos desta partilha é muito baixa. Existe uma fraca sensibilização dos utilizadores sobre como proteger a sua informação pessoal nas redes sociais, e nem sempre têm uma ideia clara sobre quem tem acesso a ela, ou como esta poderá ser usada.

Paralelamente ao crescimento imbatível dos sites de redes sociais e das crescentes preocupações com a segurança decorrentes do seu uso, temos a adicionar o advento impressivo dos dispositivos móveis, que dispondo de novas tecnologias vêm criar problemas acrescidos de segurança e privacidade, ao coletar e disponibilizar informação privada dos utilizadores nas redes sociais, em concreto a localização geográfica.

A grande questão de partida deste projeto é: **como é que os estudantes universitários percecionam as redes sociais e aquilo que expõem online, através dos seus comportamentos, opiniões ou outras partilhas?** Daqui decorre outra questão não menos relevante: **como é que estes representam, a importância desta exposição, na sua esfera de privacidade e segurança?**

Em suma, a presente pesquisa visa, sobretudo, compreender como é que os estudantes universitários percecionam o modo como se expõem online e a importância que isso tem na sua privacidade e na segurança da informação partilhada nas redes sociais.

1.5. Abordagem metodológica

Esta investigação compreendeu dois estudos em fases subsequentes, a primeira fase composta por um estudo exploratório e a segunda por um estudo inferencial e correlacional.

No estudo exploratório, de índole mais qualitativa, foi desenvolvido um *focus group* com estudantes universitários e foram feitas entrevistas com especialistas. Para o *focus group* foi desenvolvido um guião que relacionou as perguntas com os objetivos propostos. Os dados recolhidos, tanto do *focus group* como das entrevistas, foram alvo de tratamento por meio de *software* de análise de texto não estruturado. As entrevistas com os especialistas foram também baseadas num guião, mais incisivo, com vista a validar e

ampliar os dados reunidos no *focus group*. Nesta primeira fase foi possível proceder ao levantamento de conceitos e à obtenção de indicadores.

Na segunda fase foi desenvolvido um estudo inferencial, de caráter mais quantitativo. Neste segundo estudo foi construído um questionário, que teve como base não só indicadores advindos da revisão de literatura/levantamento teórico-conceptual, mas também, e sobretudo, dos resultados obtidos na fase exploratória. O questionário foi implementado em plataforma online e dirigido a estudantes universitários, tendo sido distribuído tanto por redes sociais como por intermédio de serviços de apoio administrativo e de comunicação, de diversas instituições de ensino superior em Portugal.

Os dados recolhidos foram alvo de tratamento estatístico, nomeadamente descritivo, para a caracterização da amostra, em seguida foram efetuadas análises de componentes principais para a composição das dimensões, visando os objetivos deste estudo, e feitas análises de correlações das dimensões encontradas.

1.6. Estrutura e organização da dissertação

A presente investigação está organizada por uma introdução geral seguida de duas partes compostas por sete capítulos que pretendem refletir as diferentes fases até à sua conclusão.

A primeira parte é composta pela revisão de literatura, sendo a segunda parte reservada para o estudo empírico.

O primeiro capítulo introduz o tema da investigação e objetivos da mesma, bem como uma breve descrição da estrutura do trabalho.

O segundo capítulo reflete o enquadramento teórico, designado por revisão de literatura.

O terceiro capítulo é dedicado à apresentação da investigação realizada, refere-se o processo de recolha e tratamento de dados bem como os métodos de análise utilizados em cada uma das fases da investigação, assim como a apresentação em detalhe dos objetivos do trabalho.

O quarto e quinto capítulos descrevem em detalhe os dois estudos que foram conduzidos, no quarto capítulo temos o primeiro estudo relacionado com a fase exploratório e no quinto capítulo o segundo estudo relativo à fase quantitativa.

No sexto capítulo são analisados os resultados obtidos. Seguido do sétimo capítulo composto pelas conclusões deste trabalho bem como recomendações, limitações e trabalhos futuros.

Capítulo 2 – Revisão de Literatura

2.1. Redes Sociais

2.1.1. Sociedade em Rede

Sociedade em rede, termo criado por Jan Van Dijk em 1991, mais tarde desenvolvido por Manuel Castells em 1996, na sua trilogia "A Era da Informação", é uma definição de sociedade que estende e dá toda uma nova dimensão ao conceito de rede social, isto porque, as redes sociais são na realidade formas de organização da sociedade muito antigas, bem anteriores à era da revolução da tecnologia de informação (Castells, 1996).

Jan Van Dijk define a sociedade em rede como "uma sociedade em que a combinação de redes sociais e dos média molda o seu modo principal de organização e as suas estruturas mais importantes a todos os níveis (individual, organizacional e social)" (Van Dijk, 2012, p. 26), comparando este tipo de sociedade com uma sociedade de massas moldada por grupos, organizações e comunidades – massas – organizadas numa presença física. Sendo a comunicação cara-a-cara gradualmente substituída por comunicação de redes pessoais e sociais suportadas por tecnologia digital.

Para Manuel Castells a sociedade em rede é uma nova morfologia das sociedades, pois embora as sociedades tenham estado organizadas sob a forma de rede noutros tempos e lugares, o novo paradigma da tecnologia de informação providencia os meios para a massificação e expansão em toda a estrutura social, moldando as operações e os processos de produção, experiência, poder e cultura.

Uma sociedade em rede é uma sociedade onde as principais estruturas e atividades sociais estão organizadas em torno de redes de informação digitais. Deixando de se tratar apenas de redes ou de redes sociais, passando a ser redes sociais que processam e gerem informação assentes em tecnologia microeletrónica (Castells, 2002).

De acordo com Castells as redes tornam-se na unidade básica da sociedade moderna, neste ponto Van Dijk é menos radical defendendo que apesar de tendencialmente ligados em rede, os indivíduos, os grupos, as organizações e as comunidades continuam a ser os pilares da sociedade moderna.

A sociedade em rede vai muito para além da sociedade de informação como habitualmente proclamada, as sociedades modernas não se podem definir só por tecnologia, estão também presentes fatores políticos, económicos e culturais que

compõem a sociedade em rede. Influencias como religião, educação cultural, organizações políticas e status social moldam a sociedade em rede.

As redes são estruturas abertas, capazes de se expandir de forma ilimitada, desde que a comunicação com os novos nós dentro da rede seja possível, para isso é necessário que todos os nós partilhem os mesmos códigos de comunicação (valores, princípios, gostos, religião, etc.). Uma estrutura social assente em rede pode ser um sistema altamente dinâmico, aberto e suscetível de inovação. Esta organização social em rede têm sido um dos condutores da economia capitalista, baseada em inovação, globalização e concentração descentralizada.

No período da história que se atravessa assistimos a uma ampla destruturação das organizações, deslegitimação das instituições, enfraquecimento de importantes movimentos sociais e por expressões culturais efémeras, tornando-se a identidade como a principal fonte de significado. Cada vez mais as pessoas organizam o seu significado não em torno do que fazem, mas com base no que são ou acreditam ser. Por outro lado, as redes ligam e desligam seletivamente os indivíduos, tornando-se a sociedade gradualmente numa estrutura bipolar entre a Rede e o *Self* (Castells, 2002).

No final do século XX assistimos à terceira revolução industrial (Figura 1) a revolução da tecnologia de informação, esta revolução assenta no novo paradigma das tecnologias de informação. A terceira revolução industrial tem o potencial de ser tão disruptiva como foi a primeira, pois estamos perante uma transformação radical não só do processo industrial, mas principalmente da cultura da sociedade moderna a todos os níveis.

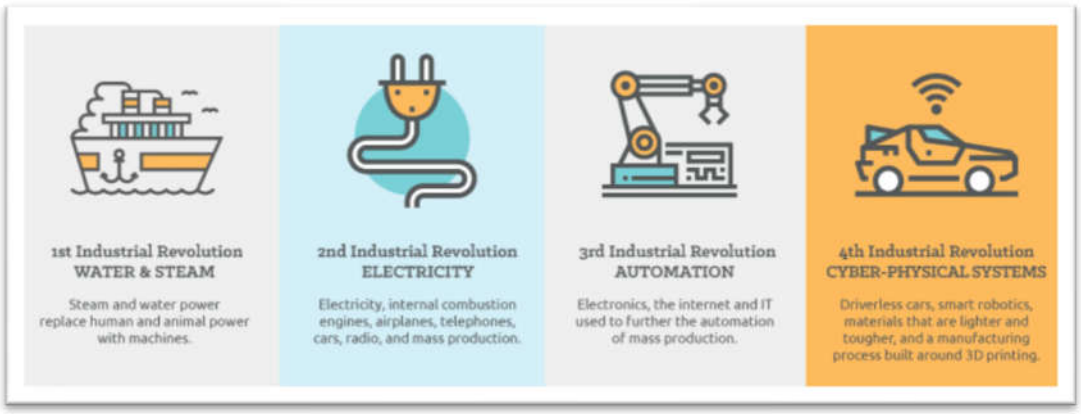

Figura 1 - As quatro revoluções industriais (Ray, 2017)[1]

[1] Imagem retirada do site: https://www.linkedin.com/pulse/future-jobs-employment-post-fourth-industrial-revolution-tanmoy-ray

A transformação da organização social decorrida da terceira revolução industrial é catapultada pelos novos média, novos métodos de comunicação num mundo digital que vêm permitir a criação de grupos de indivíduos que se reúnem num espaço digital (online) com vista a trocar bens e informação. Além da criação de comunidades virtuais, os novos média vêm dar voz aos indivíduos nas suas comunidades e no mundo. Os novos média caraterizam-se pelo uso de tecnologias de telecomunicação, pela interatividade e pela digitalização.

A sociedade em rede é então uma estrutura social baseada em redes possibilitadas por tecnologias de comunicação e informação suportadas por redes digitais de computadores que geram, processam e distribuem informação através dos nós das redes.

Os conceitos introduzidos por Jan Van Dijk e Manuel Castells da sociedade em rede são corporificados em muita da tecnologia digital hoje existente, sites de redes sociais, sistemas de mensagens instantâneas e o próprio e-mail são exemplos fundamentais da sociedade em rede em funcionamento. O âmbito das tecnologias da sociedade em rede é global e ao mesmo tempo local, é "glocal" (Wellman, 2004).

Nos primeiros anos da sua existência global, a Internet parecia pressagiar uma nova era de libertação. Os governos demonstraram incapacidade no controlo dos fluxos de comunicação que transcendiam as fronteiras políticas. A liberdade de expressão podia estender-se por todo o planeta sem depender dos meios de comunicação de massas, já que a Internet permitia a comunicação de muitos para muitos sem entraves. A privacidade estava protegida pelo anonimato da comunicação na Internet, assim como pela dificuldade de encontrar as fontes e identificar o conteúdo das mensagens transmitidas por meio dos protocolos da Internet. A transformação da liberdade e da privacidade na Internet é consequência direta da sua comercialização. A necessidade de assegurar e identificar a comunicação na Internet para poder ganhar dinheiro graças à rede e a necessidade de proteger os direitos da propriedade intelectual na mesma, resultaram no desenvolvimento de novas arquiteturas de *software* que possibilitaram o controlo da comunicação informática (Castells, 2002).

Como em muitos casos, a tecnologia é de certa forma uma espada de dois gumes, apesar de ampliar as vidas das pessoas de variadíssimas formas, à medida que o mundo se torna numa "sociedade de informação" também se levantam novas preocupações. Muita desta informação não diz respeito apenas a "coisas", mas sim a pessoas e esta informação é acedida, arquivada, manipulada, extraída, partilhada, comprada e vendida,

analisada, potencialmente perdida, roubada ou mal utilizada por números governos, corporações, agências privadas e públicas, muitas vezes sem qualquer conhecimento ou consentimento (Buchanan, Paine, Joinson, & Reips, 2007).

2.1.2. Redes Sociais Online

Numa abordagem simplista uma rede social online é uma comunidade baseada na Internet onde indivíduos interagem, muitas vezes através de perfis que representam a sua *persona* pública (e a sua rede de conexões) aos outros (Acquisti & Gross, 2006).

Grande parte dos mecanismos que compõem atualmente uma rede social online moderna foram concretizados muito antes nos anos 60 (Gross & Acquisti, 2005). Conceitos como, e-mail, salas de conversação (*chat rooms*), quadros de mensagens (*message boards*), fóruns, mensagens instantâneas (*instante messaging*), partilha remota de ecrã (*remote desktop*) e jogos multijogador já eram usados de forma integrada num projeto iniciado em 1960 na Universidade de Illinois denominado PLATO[2]. Contudo o crescimento exponencial, interesse comercial e sucesso das redes sociais online só surgiu após o advento da massificação da Internet em 1995.

O primeiro sistema reconhecido como uma rede social online foi lançado em 1997 (Figura 2), o SixDegrees.com, este site permitia aos utilizadores a criação de perfis, compor listas de Amigos e navegar pelas listas de Amigos dos seus contactos (Boyd & Ellison, 2007). Antes do SixDegrees.com outras plataformas tinham oferecido a possibilidade de criar perfis ou de suportar listas de amigos (ICQ, AIM, Classmates.com), contudo, até então não tinha ainda existido um sistema que combinasse ambas as funcionalidades (Boyd & Ellison, 2007).

O nome *Six Degrees* tem origem na teoria dos seis graus de separação originalmente concebida pelo escritor húngaro Frigyes Karinthy no seu pequeno conto com o nome *Chains* em 1929. Esta teoria preconiza que todos os seres vivos do mundo estão a seis passos ou menos uns dos outros, de tal forma que através de uma *corrente* de "amigo de amigo" podem ser relacionadas quaisquer duas pessoas num máximo de seis elos.

Anos mais tarde, em 1967 foi conduzida uma experiência denominada "Problema do Pequeno Mundo" esta experiência teve como objetivo medir e comprovar a teoria dos

[2] PLATO - Programmed Logic for Automatic Teaching Operations: Ferramenta de educação baseada em computador.

seis graus de separação aplicada sobre a população dos Estados Unidos, a conclusão da experiência foi que as pessoas nos Estados Unidos estavam ligados por aproximadamente três laços de amizade (Travers & Milgram, 1969).

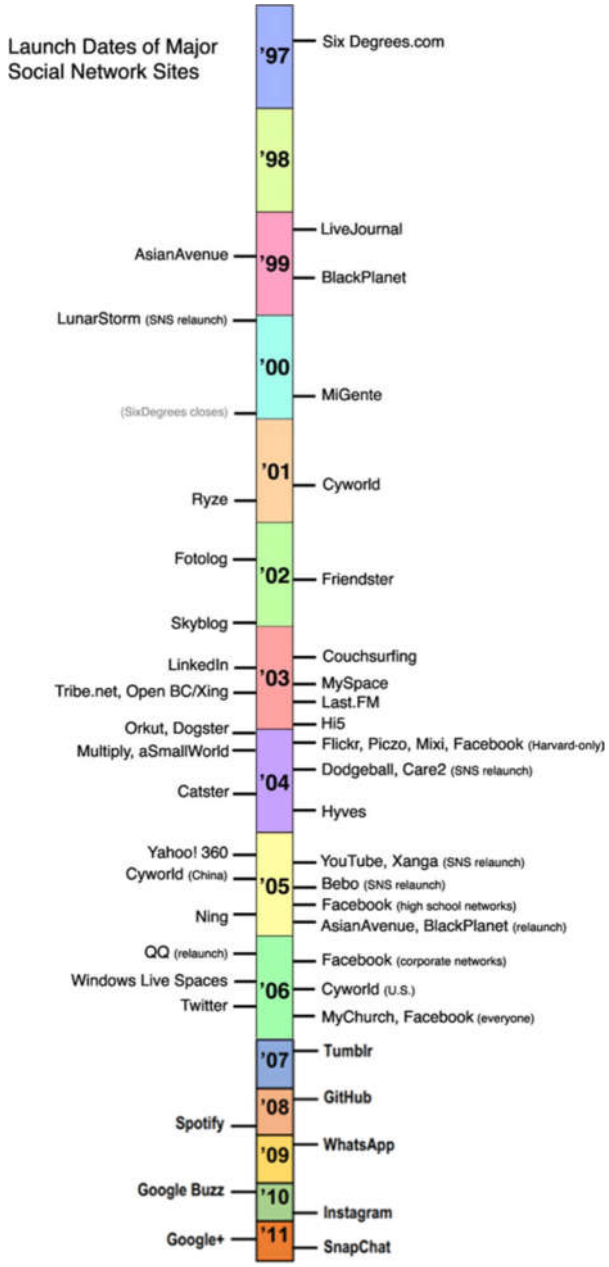

Figura 2 - Cronograma das datas de lançamento dos maiores SNS.[3]

Para além da frase popular "o mundo é mesmo pequeno", o advento das tecnologias de informação tornou o conceito subjacente aos "seis graus de separação" não só muito atrativo como particularmente viável. Em 1990 o dramaturgo John Guare escreveu uma

[3] Cronograma atualizado sobre cronograma original do artigo - *Social network sites: Definition, history, and scholarship* (Boyd & Ellison, 2007).

peça para teatro eponímia, após três anos a peça foi adaptada ao cinema e assim em 1993 é lançado o filme "Seis Graus de Separação".

Apesar do conceito existir desde 1929, foi John Guare em 1993 que popularizou a teoria dos seis graus de separação, foi esta difusão através da cultura popular que certamente terá agilizado o aparecimento em 1997 da primeira rede social denominada SixDegrees.com.

A SixDegrees.com promoveu-se como uma ferramenta para ajudar as pessoas a ligarem-se e comunicarem com outras pessoas, apesar de ter atraído milhares de utilizadores, falhou na missão de encontrar um modelo de negócio sustentável tendo encerrado em 2000, em certa medida a SixDegrees.com estava à frente do seu tempo (Boyd & Ellison, 2007).

Em 2001 assistimos a uma nova vaga de redes sociais online com o aparecimento da rede social Ryze.com, esta rede tinha como missão a alavancagem de relações entre parceiros de negócios. Futuras grandes redes como o Tribe.net o LinkedIn e o Friendster surgiram do mesmo grupo que estava por detrás da Ryze.com. A grande explosão no aparecimento de redes sociais ocorre em 2003, é nesta altura que se assiste a uma diversificação e especialização das inúmeras redes sociais online: ênfase nas redes profissionais, como são exemplos o LinkedIn, Visible Path e o Xing; redes centradas na partilha de interesses específicos como o Dogster; redes orientadas para o ativismo como o Care2; redes direcionadas para a partilha de experiências como o *Couchsurfing* e por fim as redes centradas na partilha de média com exemplos como o Flickr, o Last.FM e o YouTube (Boyd & Ellison, 2007).

Com a abundância de redes sociais online assiste-se a uma regionalização da penetração das redes pelo globo, redes como a Orkut (Google) que é um sucesso no Brasil, falha em ganhar tração noutros países, a rede Hi5 com uma grande taxa de penetração em pequenos países da América Latina e Europa (com particular incidência em Portugal), mas que não convence no resto do mundo (Boyd & Ellison, 2007).

Ao contrário das redes sociais online anteriores que tinham como objetivo a massificação, o Facebook foi inicialmente desenhado para suportar apenas comunidades colegiais. Em 2004 o Facebook começou por ser um site de rede social online restrito à comunidade académica da Universidade de Harvard. Mais tarde começou a suportar outras escolas, continuando a ser uma rede social de nicho, é esta perceção de rede social

online "fechada" ou exclusiva que contribuiu para o desenvolvimento de uma comunidade mais intimista e privada. Mais tarde em 2006 o Facebook acaba por ser lançado em acesso aberto. De forma diferenciada relativamente às outras redes socais online, o Facebook não permitia que os utilizadores colocassem os seus perfis integralmente públicos. Outra das funcionalidades diferenciadoras do Facebook foi a possibilidade de programadores externos poderem desenvolver aplicações que permitiam não só a interação com os perfis dos utilizadores como providenciavam outras funcionalidades, expandido em múltiplas formas as possibilidades de uso do Facebook (Boyd & Ellison, 2007), um exemplo muito popular disso foi o jogo FarmVille.

Em 2009 o Facebook tornou-se a rede social online mais popular e em Setembro de 2014 reportava ter 1,35 mil milhões de utilizadores mensais ativos, o que à data representava 18% da população mundial (Zlatolas, Welzer, Heričko, & Hölbl, 2015).

Uma possível definição em 2007 para uma rede social online é um serviço baseado na Internet que permite indivíduos a (1) construir um perfil público ou semipúblico dentro de um sistema delimitado, (2) articular uma lista de outros utilizadores com quem compartilha uma conexão, e (3) visualizar e percorrer a sua lista de conexões bem como as listas de conexões de cada um dos utilizadores com quem se conectam (Boyd & Ellison, 2007).

Num contexto mais recente e já totalmente imbuído na corrente Web 2.0[4] é importante identificar que o panorama das redes sociais online mudou muito desde 2007, atualmente muitas redes, permitem aos seus utilizadores a criação de listas de contactos e "Amigos", tornando esta caraterística demasiado vaga para permitir definir uma rede social online. Por outro lado funcionalidades como o "News Feed" do Facebook assente em fluxos de média, tornaram-se prevalentes na experiência dos utilizadores de redes sociais online (Ellison & Boyd, 2013).

Inicialmente as redes sociais online estavam centradas sobre o conceito de perfil, organizados à volta de um conjunto de perfis que representavam os utilizadores dessas redes, com o passar do tempo as redes sociais online foram providenciando funcionalidades que possibilitavam uma atualização mais simples e rápida destes perfis,

[4] Web 2.0: A revolução no negócio da indústria de computadores causada pela mudança para a internet como plataforma e uma tentativa de entender as regras para o sucesso nessa nova plataforma. O mote principal entre essas novas regras é: criar aplicações que aproveitem os efeitos da rede de forma a melhorarem à medida que cada vez mais pessoas as usarem "aproveitando a inteligência coletiva" (O'Reilly, 2006) Retirado do site: http://radar.oreilly.com/2006/12/web-20-compact-definition-tryi.html

o perfil passou de uma mensagem de autoapresentação para passar a ser um retrato do individuo com a sua expressão de ação. Estas funcionalidades vieram combater um dos problemas emergentes das redes sociais online, os perfis – ficavam envelhecidos e parados no tempo, assemelhando-se a espaços abandonados (Ellison & Boyd, 2013).

Atualmente as redes sociais online comportam-se mais como agregadores de notícias do que com contextos centrados em perfis. Em algumas redes sociais online, o "perfil" pode estar totalmente diluído na atividade do utilizador e na sua lista de contactos, não existindo qualquer tipo de informação bibliográfica tradicionalmente associada ao perfil.

Os perfis de hoje deixaram de ser simplesmente auto descritivos, contendo texto estático, passaram a ser uma combinação dinâmica de conteúdo alimentado pelos utilizadores, relatórios de atividades, conteúdo providenciado por outros e/ou conteúdo fornecido pelo próprio sistema (Ellison & Boyd, 2013).

Inicialmente as listas de amigos eram predominantemente recíprocas, isto é, uma ligação entre duas pessoas só era instanciada quando ambas as partes concordassem. À medida que o Twitter cresceu, também a noção de que poderiam existir relações unidirecionais em que pessoas seguem outras pessoas sem reciprocidade também cresceu. Ainda em relação à questão das listas de "Amigos", existe a questão do "colapso de contexto" em que pessoas têm na sua lista de contactos pessoas de diversos contextos (familiar, profissional, membros de igrejas, etc.), tornando desconfortável a presença na rede social online (Ellison & Boyd, 2013).

Em linha com estes novos paradigmas surge a nova definição de uma rede social online, é uma plataforma de comunicação em rede onde os seus participantes (1) dispõem de perfis únicos compostos por conteúdo fornecido pelos próprios, conteúdo fornecido por outros utilizadores e/ou informação providenciada pelo sistema; (2) podem articular conexões públicas que podem ser vistas e percorridas por outros; e (3) podem consumir, produzir e/ou interagir com fluxos de conteúdo gerado pelos utilizadores presentes nas suas conexões (Ellison & Boyd, 2013).

2.2. Exposição online e *Social media*

2.2.1. Autoexposição

Uma parte significativa da rotina diária de muitos utilizadores da Internet passa pelo uso das redes sociais online, o uso destes sistemas oferece a possibilidade de encontrar amigos e manter o contacto de forma rápida e eficiente.

Atualmente existem ambientes organizacionais e de *software* que controlam a troca de informações interpessoais em redes sociais online, mensagens de texto, aplicações de mensagens instantâneas, jogos multijogador online, aplicações de trabalho colaborativo e educação online. Todas estas aplicações fazem parte da chamada *social media*, ou média que apoia a colaboração social. O termo *social media* é na realidade um conceito agregador que descreve *software* social[5] e redes sociais (Barnes, 2006; Kaplan & Haenlein, 2010).

Frequentemente as redes sociais online oferecem novas ferramentas para ajudar a construir e manter estas relações sendo assim de particular importância para o desenvolvimento psicológico. Aliás, muitas das funcionalidades base destas plataformas estão explicitamente desenhadas para facilitar a criação e manutenção de conexões entre pessoas através da autoexposição[6] de informação (Hallam & Zanella, 2017).

Nas gerações mais recentes, os "Millennials" e os "Post-Millennials"[7], são/foram jovens que apesar de terem as mesmas necessidades sociais que as gerações anteriores, vêem-se forçados a crescer num mundo em que o perigo e o conflito estão em todo o lado. Resultado disso, a sua liberdade de movimentos é bastante reduzida pelos seus progenitores e pelos seus próprios medos de insegurança. Contudo ao tentarem forjar as suas identidades em espaços seguros, os adolescentes usam as redes sociais online como "recreios" para experimentar e se emanciparem longe do escrutínio dos adultos (Boyd, 2014).

[5] *Software* social refere-se a vários tipos de aplicações vagamente conectados que permitem que os indivíduos se comuniquem uns com os outros e acompanhem discussões na Internet à medida que acontecem.
[6] Autoexposição pode ser definida como o ato de revelar informação pessoal junto de outros (Zlatolas et al., 2015).
[7] Geração Z ou Geração Internet – Indivíduos nascidos entre 1990 e 2010, a primeira geração a ter acesso generalizado à Internet desde tenra idade.

Por outro lado, a capacidade das redes sociais online promoverem a criação de capital social[8] em particular relações do tipo "laços fracos". A Internet só por si não compreende a acumulação de capital social, mas o uso intensivo de redes sociais online sim, contribui comprovadamente para a criação e acumulação de capital social (Ellison, Steinfield, & Lampe, 2007). Esta acumulação de capital social facilita a manutenção de relações à medida que as pessoas se movem de uma comunidade *offline* para outra. As relações online não removem necessariamente as pessoas do seu mundo *offline*, aliás podem até ser usadas para suportar relacionamentos e manter pessoas em contacto.

Apesar dos aspetos positivos das redes sociais online, estas plataformas são frequentemente alvo de alertas por parte de grupos, *bloggers* e outros média online pelos riscos de privacidade que potenciam para os seus utilizadores que recorrem muitas vezes à partilha excessiva de informação (Boyd, 2008).

Esta partilha desregrada de informação nas redes sociais online pode muitas vezes ser causa e consequência de comportamentos de adição, a manutenção de intensa atividade em redes sociais online despoleta sentimentos de atração pelo próprio, pessoas com elevados traços de narcisismo tendem a ser mais ativas nas redes sociais online, já que estas plataformas oferecem a oportunidade de apresentar-se de uma forma mais favorável, de acordo com o "eu" ideal. A incidência de casos de dependência pelo uso de redes sociais online é já de tal forma frequente que existe uma escala para a medição destes casos por forma a ajudar os profissionais de saúde a identificar situações fora do regular, esta escala é conhecida por BFAS[9] (Andreassen et al., 2012).

Os indivíduos que dispõem de perfis em redes sociais online tomam atitudes de maior risco de exposição comparativamente com os que não possuem perfis em redes sociais online (Fogel & Nehmad, 2009).

Não obstante o escrutínio que as redes sociais online têm sofrido, a introdução de mecanismos de restrição de acesso, o aumento de medidas restritivas e politicas mais rígidas de privacidade por forma a protegerem contra o uso não autorizado de informação colocada online, as vidas privadas serão cada vez mais vividas no domínio público com

[8] Capital social refere-se em larga escala à soma dos recursos, reais ou virtuais, que se acumulam para um indivíduo ou um grupo em virtude de possuir uma rede duradoura de relações mais ou menos institucionalizadas de conhecimento e reconhecimento mútuo (Ellison et al., 2007).
[9] BFAS – The Bergen Facebook Addiction Scale

a perda de uma expectativa razoável de proteção da privacidade para a informação pessoal (Rosenblum, 2007).

Contudo, apesar dos riscos da partilha de informação pessoal de forma não controlada nas redes sociais online, tendencialmente assiste-se a uma partilha cada vez maior e mais detalhada de informação privada. Dos jovens[10] que usam redes sociais online 91% partilha fotos suas, 71% divulgam o nome das suas escolas, 71% colocam a cidade onde vivem, 53% divulgam o seu endereço de email e 20% partilham o seu número de telemóvel (Madden, Lenhart, & Cortesi, 2013), esta crescente tendência de autoexposição excessiva tem-se vindo a acentuar.

Alguns dos fatores que influenciam a autoexposição estão relacionados com: o tempo gasto nas redes sociais online; o número de "amigos"; a perceção dos riscos; os benefícios; a manutenção de relacionamentos; a coesão social; a personalidade; o prazer; a curiosidade; ou simplesmente para passar o tempo (Zlatolas et al., 2015).

A autoexposição é na realidade resultado do processo consciente de equilíbrio entre os riscos e os benefícios da divulgação da informação (Krasnova, Kolesnikova, Guenther, & Günther, 2009). Ainda assim a gratificação é clara e imediata, já os riscos de privacidade são difíceis de avaliar, levando o utilizador a usar o argumento "isso não vai acontecer comigo" para explicar o comportamento de *oversharing*[11] (Krasnova et al., 2009).

Vulgarmente denominados "*digital natives*", a Geração Internet nasceu no território – ainda por cartografar – da Internet e dos *social media*, ficando assim mais vulneráveis à ingenuidade e ao erro (Boyd, 2014). Esta ingenuidade está particularmente ligada à falsa ilusão de privacidade e segurança que muitos jovens assumem que a Internet dispõe, será mesmo caso para poderem ser apelidados de "*digital na(t)ives*" (Hargittai, 2010). Não se pode assumir que os jovens estão automaticamente mais informados em virtude da sua "natividade digital". Existe uma miríade de casos de sentimentos magoados, embaraçamentos, humilhações, danos à reputação e pior… derivados da exposição e divulgação pública de conversas privadas, informação ou fotos espalhadas "por aí" as quais não será possível recolher ou alterar (Boyd, 2014), tudo isto por se usar as redes sociais online como se fossem diários pessoais (Rosenblum, 2007).

[10] Entre os 12 e os 17 anos de idade.
[11] *Oversharing*: Revelar uma quantidade inadequada de detalhes sobre a própria vida pessoal. Retirado do site https://en.oxforddictionaries.com/definition/overshare

As redes sociais online são imensuravelmente mais vastas e mais vagas comparativamente com as redes sociais *offline*. É possível o perfil de um utilizador estar ligado diretamente a centenas de outros utilizadores e de forma indireta a milhares deles. Muitos dos contactos que fazem parte da lista de "amigos"[12] dificilmente o serão na vida real, de facto muitos deles são completos estranhos! Alguns adolescentes aceitam pedidos de amizade de estranhos apenas na tentativa de aumentar o número total de amigos nos seus perfis e assim parecerem populares (Rosenblum, 2007). Mesmo assim informação pessoal e muitas vezes sensível é colocada na rede de forma despreocupada, livre e pública (Gross & Acquisti, 2005).

2.2.2. Perceção de partilha de informação

A recolha de dados pessoais identificáveis por parte de uma plataforma online é percecionada como justa apenas quando é dado o controle da informação ao utilizador, sendo este informado sobre as intenções de uso desta informação por parte do sistema, desta forma é possível caraterizar a noção de perceção de privacidade dos utilizadores da Internet em três fatores, em concreto: recolha, controlo e consciência das práticas de privacidade (Malhotra, Kim, Agarwal, Tech, & Peachtree, 2004).

Por recolha entende-se o ato de coleta de dados propriamente dito, podendo ser lícito ou ilícito, este fator é o ponto de partida primordial para muitas das preocupações com a privacidade; Controlo é a capacidade percecionada dos utilizadores na sua possibilidade de gerirem toda a informação privada que partilham com uma determinada plataforma online; Consciência das práticas de privacidade, ao contrário do controlo e da recolha, a consciência das práticas de privacidade é uma dimensão passiva da privacidade de informação, diz respeito ao nível de preocupação do utilizador relativamente às práticas de privacidade da organização que detém a plataforma online (Malhotra et al., 2004).

É a confiança na capacidade de controlar a informação e o seu fluxo nas redes sociais online que leva os utilizadores a estabelecer a sua perceção de gestão de privacidade. Contudo existem dicotomias significativas entre as preocupações com a privacidade e os efetivos comportamentos relativos à revelação de informação (Acquisti & Gross, 2006).

[12] «Num mundo onde as amizades são mediadas por interfaces digitais, a amizade pode ser definida como a regularidade com que se visita o perfil de outra pessoa» (Rosenblum, 2007).

A perceção sobre a proteção da privacidade de um site é o nível no qual os seus utilizadores sentem que esse site protege a sua privacidade, esta perceção tem impacto direto na confiança que é depositada no site (Metzger, 2006).

O conceito de perceção de segurança é diferente do conceito de confiabilidade. A confiabilidade de um site é o quanto os seus utilizadores confiam no site baseado em fatores como o reconhecimento da marca, capacidade de entrega do serviço e proteção contra a fraude. Na maioria dos casos um site ganha confiabilidade baseando-se na sua performance de longo prazo e através do boca-a-boca dos seus utilizadores. Já a perceção de segurança lida com a sensação de segurança dos utilizadores no exato momento em que estes estão ligados no site, não é um conceito adquirido ao longo do tempo, depende apenas da informação de segurança que é apresentada ao utilizador enquanto este está conectado na plataforma (Yenisey, Ozok, & Salvendy, 2005).

Os utilizadores ao criarem perfis nas redes sociais online estão de certa forma, e de um modo consciente, a escolher um certo nível de transparência. As comunidades online encorajam a partilha aberta, por isso apesar de existirem controlos de privacidade, muitos utilizadores publicam de forma pública (Rosenblum, 2007). Informações pessoais são fornecidas de bom grado sem uma ideia clara de quem tem acesso à informação ou como é que ela pode ser usada, para além disso as configurações de privacidade da maioria das redes sociais online são consideradas permissivas (Krishnamurthy & Wills, 2008).

Apesar de se presumir que todos os indivíduos com literacia digital[13] e meios usam a Internet no seu dia-a-dia, são muitas as diferenças na forma como estas pessoas incorporam o uso do "online" no seu quotidiano. Idade, género, raça/etnia, educação, rendimento, situação de emprego e local de residência são alguns dos fatores que podem explicar as diferenças de uso da Internet (Hargittai, 2010). Por exemplo, indivíduos com níveis de educação superiores são mais propensos a usar a Internet em busca de informação relacionada com saúde, envolverem-se em transações financeiras, pesquisar e procurar por emprego e recolher notícias, em contraste, níveis de educação mais baixos são mais propensos a usar a Internet de forma mais lúdica (Hargittai, 2010). Outro preditor do uso da Internet é a experiência, a experiência pode ser entendida de duas formas (1) o número de anos em que alguém está "online"; e (2) a quantidade de tempo que uma pessoa gasta "online" (Hargittai, 2010).

[13] Literacia digital - Conhecimento individual sobre funções relacionadas com computador (Park, 2013)

Os indivíduos da Geração Internet, por razões de oportunidade e conjuntura, dispõem de um elevado nível de experiência com o "online" e, por conseguinte, mais propensos à partilha de informação. Apesar da maior quantidade de partilha de informação, estas camadas mais jovens não são imunes às preocupações com as potenciais ameaças de privacidade (Park, 2013).

A perceção de partilha e privacidade de informação é resultado direto da perceção de controlo e facilidade de acesso à informação, uma rede social online que disponha de mecanismos que permitam ao utilizador configurar e definir os parâmetros de partilha de uma forma simples e óbvia contribui de forma fulcral para o aumento da confiança no sistema e por conseguinte num aumento da perceção de segurança e privacidade (Hajli & Lin, 2016; Hoadley et al., 2010), mesmo de forma "ilusória".

Por outro lado, a alfabetização digital por si só não promove uma maior perceção na partilha da informação, os utilizadores digitalmente literatos são muitos estratificados e estão longe de serem competentes no exercício do controle de privacidade. Além disso, enquanto o conhecimento desempenha um papel crítico no comportamento da privacidade, os níveis de compreensão das práticas de vigilância comuns dos sites continuam a ser irrisórios entre a maioria dos utilizadores. Contudo, a literacia digital, por vezes, desempenha um papel importante na promoção de comportamentos mais restritivos na partilha de informação privilegiada nos sites online (Boyd & Hargittai, 2010; Park, 2013). Em suma alguns utilizadores estão melhor posicionados a exercer esse controlo, enquanto que outros permanecem incapazes de o desempenhar.

Privacidade é conceptualizada como a restrição no acesso à informação, mas participar em *social media* requer partilha de informação. Para existir online, as pessoas têm de contribuir com texto, fotos, *likes*, favoritos e comentar os conteúdos de outras pessoas para que ambas se reconheçam e envolvam com outros. O ato de partilhar é central na participação no *social media*. Partilhar em *social media*, geralmente significa contribuir com conteúdo para um ecossistema persistente e amplamente acessível, muitas vezes assumido como um ato de publicidade sem governo por conceções de privacidade (Marwick & Boyd, 2014).

2.3. Confiança, Segurança e Privacidade

2.3.1. Preocupações de Confiança e Privacidade

Para a comunicação cara-a-cara a confiança é algo critico para possibilitar a partilha de informação e o desenvolvimento de novas relações, para interações online bem-sucedidas a confiança é algo também muito importante (Dwyer, Hiltz, & Passerini, 2007).

Confiança é a disponibilidade de um partido ficar vulnerável às ações de outra parte baseada na expectativa que a outra parte irá desempenhar uma ação importante para o fiduciário, independentemente da capacidade de verificar ou controlar a outra parte (Dwyer et al., 2007; Shin, 2010).

A teoria da troca social assenta numa análise de custo-benefício em relação à interação social. Se a troca for percebida como benéfica, então o individuo provavelmente entrará numa relação de troca. A confiança é usada no cálculo da perceção do custo. Alta confiança leva a uma perceção de baixo custo e vice-versa. Estudos de situações de intercâmbio interpessoal confirmam que a confiança é uma condição prévia para a autoexposição e a partilha de informação privada, porque reduz os riscos percebidos envolvidos na revelação de informações privadas (Bergström, 2015; Chen & Chen, 2015; Dwyer et al., 2007; Metzger, 2006).

As preocupações sobre a privacidade online têm origem na capacidade da tecnologia de monitorizar e gravar quase todos os aspetos do comportamento dos utilizadores na Internet. Estes receios são ainda mais alimentados pelos sucessivos relatos de sites que violam os seus próprios acordos de privacidade distribuindo – de forma voluntária ou involuntária – informação dos seus utilizadores sem permissão (Metzger, 2006).

A digitalização da informação, associada aos custos reduzidos para o seu armazenamento, está a potenciar um aumento na capacidade de recolha, conservação e análise de dados, em particular dados pessoais. Estes dados pessoais são um insumo crucial para muitas empresas na Internet em especial as redes sociais online, como Facebook, Twitter, e o LinkedIn, cujos modelos de negócio se baseiam na exploração de dados pessoais (Cecere, Le Guel, & Soulié, 2015).

Do ponto de vista de recolha e tratamento de informação pessoal, as práticas das redes sociais online têm vindo a tornar-se cada vez mais fonte de controvérsia relativamente à preocupação do ponto de vista da privacidade, a título de exemplo em junho de 2012 um estudante de direito Australiano requereu junto do Facebook uma cópia de toda a

informação recolhida sobre ele. O Facebook enviou um documento com 1222 páginas contendo informação pessoal, tendo o aluno percebido que alguma da informação pessoal tinha sido recolhida sem o seu conhecimento e consentimento (Cecere et al., 2015).

O papel da confiança para proporcionar a partilha de informação é particularmente importante em intercâmbios online, onde a comunicação mediada por computador substitui o contato físico (Metzger, 2006). Contudo será possível aderir a uma rede de milhões de pessoas e confiar em todas elas? Isto não parece realista, uma vez que as pessoas obviamente aderem às redes sociais online e estão a revelar informações, que papel tem a confiança na utilização destas redes sociais?

Num contexto estritamente legal, privacidade é o direito de se uma pessoa ser deixada em paz (Buchanan et al., 2007; Cecere et al., 2015), no contexto das redes sociais online privacidade pode ser definida como o controle sobre o fluxo de informações pessoais, incluindo a transferência e troca dessas informações (Boyd, 2008; Cecere et al., 2015; Shin, 2010). Privacidade também pode ser proteger a informação pessoal de ser mal utilizada por entidades mal-intencionadas ao mesmo tempo que é permitido a determinadas entidades autorizadas o acesso a essa informação pessoal (Aldhafferi, Watson, & A.S.M, 2013).

Preocupação com a privacidade em contexto de redes sociais online é o desejo de manter informação pessoal fora das mãos de outros, ao mesmo tempo reter a capacidade de se conectar com outras pessoas sem interferência, de certa forma a preocupação com a privacidade é uma medida subjetiva, varia de indivíduo para indivíduo com base nas próprias perceções e valores de cada um, por outras palavras, pessoas diferentes têm diferentes níveis de preocupação acerca da sua privacidade (Buchanan et al., 2007).

A idade e o nível de educação influenciam positivamente a preocupação com a privacidade, indivíduos mais novos e mais idosos têm menores preocupações com a privacidade comparativamente com o resto da população. Pessoas com níveis de educação mais elevados têm também maiores preocupações com a privacidade (Bergström, 2015; Cecere et al., 2015). Alguns autores defendem que os homens estão menos preocupados do que as mulheres sobre a sua privacidade online (Acquisti & Gross, 2006; Bergström, 2015; Cecere et al., 2015; Hajli & Lin, 2016). Outros estudos empíricos não encontram diferenças significativas entre homens e mulheres na perceção de privacidade (Boyd & Hargittai, 2010; Park, 2013). Existe, contudo, um padrão muito específico de preocupação com a privacidade relacionado com o regime sociopolítico dos

países a que cada indivíduo pertence, na Europa (Figura 3) cidadãos pertencentes a países mais individualistas (norte da Europa e Europa oriental), apresentam menores preocupações com o mau uso da sua informação pessoal. Por outro lado cidadãos de países com altos níveis de preocupação por segurança e desconfiança nas organizações estão mais preocupados com o potencial mau uso da sua informação pessoal nas redes sociais online, Europa central e sul da Europa (Cecere et al., 2015). Quanto mais as pessoas acreditarem no direito à privacidade, mais provavelmente terão preocupações com a privacidade online (Bergström, 2015).

Figura 3 - Percentagem de indivíduos bastante preocupados ou muito preocupados com o mau uso de dados pessoais nos países europeus[14]

A privacidade nas redes sociais online geralmente não é esperada ou é indefinida (Dwyer et al., 2007). Portanto, estes sistemas necessitam de políticas explícitas e mecanismos de proteção de dados para fornecer o mesmo nível de privacidade social encontrado nas redes sociais *offline*.

[14] Fonte: Pesquisa Eurobarómetro 2009 - Perceived Internet privacy concerns on social networks in Europe (Cecere et al., 2015).

A passividade da relação entre os utilizadores e as redes sociais online relativamente às preocupações com a privacidade tem os seus limites, em 5 de setembro de 2006 o Facebook decidiu implementar a funcionalidade "*News Feeds*", basicamente era uma funcionalidade que colocava em destaque todas as interações dos utilizadores na popular rede social perante toda a sua rede de "amigos", sem qualquer hipótese de segmentação ou controlo da divulgação de informação. Após o lançamento desta funcionalidade houve literalmente uma chuva de indignação na rede social com uma elevada cobertura mediática, a hecatombe foi de tal dimensão que existem até autores que dizem que esta foi a "primeira revolução oficial da Geração Y" (Hoadley et al., 2010).

Após o traumático evento para o Facebook ao qual Mark Zuckerberg[15] respondeu com um blog intitulado "*Calm down. Breath. We Hear You*", foram desenvolvidos e implementados em tempo record (dois dias!) mecanismos de controlo de privacidade e controlo de fluxo de dados e eventos dentro da rede, cujas as fundações ainda hoje servem de base aos mecanismos atuais de gestão de privacidade e segmentação de informação do Facebook (Boyd, 2008).

A relação entre privacidade e a rede social de uma pessoa é multifacetada. Em certas ocasiões, a pessoa quer que informação sobre si seja conhecida apenas por um pequeno círculo de amigos íntimos e não por estranhos. Noutros casos, está disposta a revelar informações pessoais a estranhos anónimos, mas não ao seu círculo de pessoas mais íntimas (Gross & Acquisti, 2005).

Em última análise a confiança que cada indivíduo tem nas outras pessoas é o fator que mais influencia as preocupações de privacidade entre pessoas que usam *social media* e aplicações digitais. Quanto mais uma pessoa confia nas outras, menores são as suas preocupações com o uso indevido da sua informação pessoal (Bergström, 2015).

Com a crescente massificação dos serviços baseados na *cloud*[16] cada vez mais os utilizadores trocam privacidade por serviço (Bergström, 2015), entidades como o

[15] Co-fundador do site de rede social Facebook, ocupa atualmente os lugares de CEO e Chairman da empresa Facebook, Inc. (https://en.wikipedia.org/wiki/Mark_Zuckerberg).

[16] Termo *cloud* tem origem no campo das telecomunicações nos anos 90, onde os fornecedores de acesso à Internet começaram a usar serviços de VPN (ligações virtuais privadas) para comunicação de dados. As VPN ofereciam a mesma largura de banda que as redes fixas com um custo consideravelmente menor: por sua vez estas redes suportavam roteamento dinâmico, o que permitia uma utilização equilibrada de toda a rede e por conseguinte um aumento na eficiência da largura de banda, isto levou ao aparecimento do termo "Telecom cloud" (Kaufman, 2009).

Facebook, a Google, a Microsoft, ou a Amazon controlam a *cloud*, e o utilizador para o bem ou para o mal já entrou na carruagem (Guha, Tang, & Francis, 2008).

As preocupações de privacidade dos utilizadores das redes sociais online são principalmente determinadas pela probabilidade percecionada de uma violação de privacidade e muito menos pelo dano esperado dessa mesma violação de privacidade (Krasnova et al., 2009).

De acordo com Shin (2010) é possível usar o modelo TRA[17] (Figura 4) para explicar o padrão de adoção das redes sociais online. A adesão das pessoas às redes sociais online assenta sobre três pilares: (1) segurança, (2) privacidade e (3) confiança.

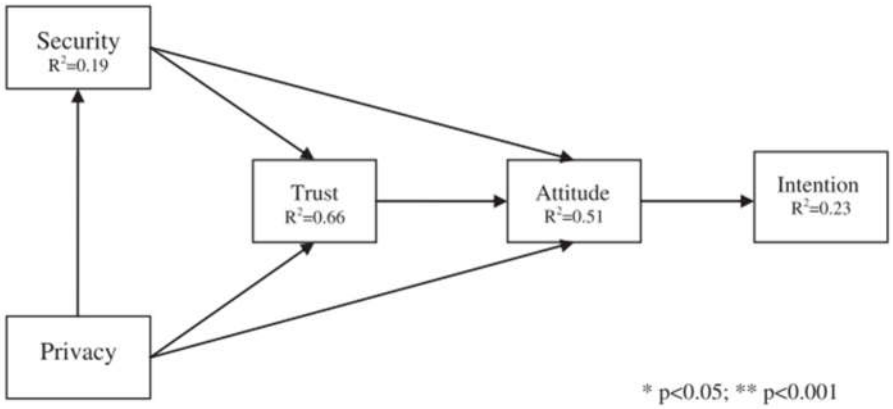

Figura 4 - Modelo TRA (Shin, 2010, p. 430)

Verifica-se desta forma que a perceção de privacidade produz um efeito positivo na perceção de segurança e que por sua vez ambas produzem um efeito positivo na perceção de confiança e é esta sinergia entre privacidade, segurança e confiança que conduz as pessoas a uma atitude que leva à intenção de aderir a uma rede social online (Shin, 2010).

2.3.2. Paradoxo da Privacidade

De acordo com o quadro do paradoxo da privacidade, indivíduos com altos níveis de preocupação sobre privacidade tendem a expor e divulgar seus dados pessoais mais prontamente (Bonneau & Preibusch, 2010; Norberg, Horne, & Horne, 2007). A revelação de informações pessoais nas redes sociais online, apesar da existência de preocupações de privacidade, é denominada de "paradoxo da privacidade" (Barnes, 2006; Krasnova et

[17] TRA – Theory Reasoned Action: define a atitude perante um comportamento como o sentimento positivo ou negativo de um individuo em relação ao desempenho do próprio comportamento. A atitude de uma pessoa em relação ao comportamento é determinada pelas suas crenças e avaliações (Shin, 2010).

al., 2009; Young & Quan-Haase, 2013). De certa forma o "paradoxo da privacidade" é o hiato entre as preocupações dos indivíduos com a privacidade e os seus comportamentos em situações relacionadas com a manutenção da privacidade (Hallam & Zanella, 2017).

A economia comportamental e as teorias psicológicas fornecem três explicações interrelacionadas para este paradoxo: (1) informação incompleta, (2) racionalidade limitada, e (3) distorção psicológica (Cecere et al., 2015). Informação incompleta implica que as pessoas não estão cientes dos possíveis riscos de invasão de privacidade. Em situações sensíveis à privacidade, a racionalidade limitada refere-se à incapacidade dos indivíduos de comparar os custos e benefícios associados à divulgação de informação privada. De um ponto de vista económico, informação incompleta combinada com racionalidade limitada dos agentes, por si só, pode estar na origem do paradoxo da privacidade (Cecere et al., 2015). A distorção psicológica implica que o comportamento individual não é consistente ao longo do tempo devido a personalidades múltiplas (Gross & Acquisti, 2005). Em particular, o desconto hiperbólico implica que as pessoas podem sobreavaliar a gratificação no curto-prazo, ou seja, o uso das redes sociais online, contra as ameaças de longo-prazo, isto é, o uso indevido de dados pessoais (Cecere et al., 2015; Hallam & Zanella, 2017). Este paradoxo – à semelhança da teoria da troca social – trata-se também de uma decisão baseada numa análise de custo-benefício (Bergström, 2015), onde os "benefícios da recompensa social" afetam diretamente o comportamento no imediato, ao invés que os "custos da preocupação com a privacidade" apenas afetam as intenções no futuro distante, que por sua vez não influencia diretamente o comportamento atual (Hallam & Zanella, 2017).

Sob certas condições, mesmo pessoas com perceções negativas sobre a divulgação de informação pessoal, irão efetivamente fornecer essa informação quando diretamente solicitada (Norberg et al., 2007).

Podem até tecer-se analogias entre o processo de tomada de decisão humana e o processo de medição de experiências quânticas, através dos efeitos da *indeterminação*, isto é, o resultado de um processo de tomada de decisão é determinado apenas no momento em que a decisão é tomada e não antes. No que toca a tomadas de decisão no âmbito da privacidade, estas poderão ser afetadas pelo efeito da *indeterminação*, uma vez que os indivíduos podem alterar as suas preferências indeterminadamente, ou seja, apenas no exato momento em que a decisão efetiva é tomada (Kokolakis, 2017).

Existe por vezes uma desconexão entre o desejo de proteger a privacidade e o comportamento, é como se o individuo (em particular os mais jovens) por momentos se esquece da natureza publica da Internet (Acquisti & Gross, 2006; Barnes, 2006; Boyd & Ellison, 2007). Embora os utilizadores estejam bastante preocupados com uma possível violação da sua privacidade, apenas uma parcela usa adequadamente as opções de privacidade disponíveis nas redes sociais para proteger a sua informação de públicos não desejados (Hallam & Zanella, 2017).

Apesar do paradoxo, os jovens dispõem de algumas estratégias para mitigar este défice de privacidade, que são usadas principalmente como proteção contra ameaças de privacidade social, e que consistem em: excluir informações de contacto, usar perfis limitados, remover marcadores, remover fotografias e limitar pedidos de amizade de estranhos (Young & Quan-Haase, 2013). Apesar destas estratégias focadas na reposição de privacidade entre os utilizadores das redes socias online, existe pouca ou nenhuma preocupação com a privacidade institucional, pelo que não são empregues quaisquer estratégias para proteção do uso indevido da informação pessoal por parte das organizações (Young & Quan-Haase, 2013).

Num programa de TV onde era discutido o tema da rede social Facebook, uma pessoa expressou a sua opinião de preocupação em divulgar informação privada na rede. Após o repórter lhe pedir se ela podia mostrar o seu perfil no Facebook, ela assim fez. O seu perfil continha a sua morada de casa, número de telefone, e uma fotografia do seu pequeno filho. Sem qualquer consciência de perigo, ela forneceu muita informação que era considerada sensível (Nagy & Pecho, 2009).

Os utilizadores publicam voluntariamente grandes quantidades de dados pessoais e sensíveis, mesmo sabendo e expressando preocupação com os riscos que as redes sociais online representam para a privacidade da sua informação (Hallam & Zanella, 2017). Apesar de parecer um contrassenso a preocupação com privacidade dificilmente afeta a divulgação de informação, outras variáveis moderam esta relação. A relevância social percecionada e o número de aplicações usadas são importantes. A vontade geral dos utilizadores de divulgar prevalece mesmo quando fornecem informações sensíveis (Taddicken, 2014).

Os jovens entendem e preocupam-se com os potenciais riscos associados à divulgação de informação nas redes sociais e desenvolvem alguns comportamentos de proteção de privacidade no *social media*. No entanto, sentem que assim que a informação é partilhada,

está fora do seu controle. Esta falta de controle é atribuída às práticas opacas das organizações responsáveis pelas redes sociais, aos recursos tecnológicos dos *social media* e ao conceito de privacidade em rede, que reconhece que os indivíduos existem em contextos sociais onde outros podem violar a sua privacidade (Hargittai & Marwick, 2016).

O enquadramento do paradoxo da privacidade aplicado às redes socias online é uma matéria relativamente antiga que remonta ao período do surgimento do Facebook, recentemente foi conduzido outro estudo confirmatório de forma a identificar se à luz das atitudes atuais nos *social media* o paradoxo ainda se verifica, e efetivamente voltou a ser validado, o paradoxo tal como foi concebido na sua génese ainda existe, contudo verifica-se que os comportamentos dos utilizadores das redes sociais online não são tão paradoxais como se acreditava (Dienlin & Trepte, 2015).

A presença simultânea de falta de conhecimento de risco e uso de comportamentos de proteção de privacidade sugere que o paradoxo da privacidade não pode ser atribuído unicamente à falta de compreensão ou à falta de interesse em privacidade. Atualmente os utilizadores apresentam uma sensação de apatia e até mesmo de cinismo quando confrontados com questões de privacidade online, especificamente acreditam que as violações de privacidade são inevitáveis e que a não participação no *social media* não é uma opção (Hargittai & Marwick, 2016).

Em ambientes socialmente muito interligados, a capacidade dos indivíduos de controlar a disseminação da sua informação pessoal é comprometida por violações tecnológicas e sociais da sua privacidade. A privacidade deixa de ser um processo individual, passando a ser um esforço coletivo que exige a cooperação de todos os nós da rede do *social media*. Poderá até dizer-se que afinal não é paradoxal os jovens desejarem partilhar informações sobre si mesmos enquanto reconhecem simultaneamente a incapacidade de soluções técnicas ou normas sociais para proteger a sua privacidade adequadamente (Hargittai & Marwick, 2016).

2.3.3. Privacy by design

O termo "*privacy by design*" refere-se à necessidade de abordar as questões da privacidade desde o início. Trata-se de uma filosofia para aprimorar o design através da

incorporação de preocupações de privacidade como requisitos em áreas de design, tais como design de tecnologia, práticas de negócio e design físico (Cavoukian, 2011).

A abordagem "*privacy by design*" é caracterizada por medidas pró-ativas e não reativas, ela antecipa e previne eventos invasivos de privacidade antes de eles acontecerem. A "*privacy by design*" não oferece remédios para a resolução de infrações de privacidade, uma vez que elas tenham ocorrido – visa evitar que ocorram. Se um utilizador nada fizer num sistema, a sua privacidade permanece intacta, não é necessária qualquer ação por parte do indivíduo para proteger a sua privacidade – ela está incorporada no sistema, por omissão. Em suma a "*privacy by design*" é primordialmente centrada no utilizador (Cavoukian, 2011).

A maioria das pessoas envolvidas no desenvolvimento de sistemas de informação, está bem ciente que projetar a segurança e privacidade (assim como praticamente todos os requisitos não funcionais de um sistema) bem no inicio do projeto é imensuravelmente melhor em oposição ao esforço de tentar adicionar estas camadas de segurança mais tarde no decorrer do projeto (Shapiro, 2010). Contudo verifica-se com alarmante frequência falhas nos mais diversos sistemas que põem em risco a privacidade e a segurança de informação privada. O caso recente mais gritante desta recorrente falta de segurança foi a brecha de segurança da Equifax[18]. Foram perdidos dados sensíveis de 143 milhões de consumidores americanos, nomes, números de segurança social, datas de nascimento, moradas e até números de cartas de condução. Além destes dados foram também usurpados números de cartões de crédito de 209 mil pessoas bem como documentos com informação de identificação pessoal de outras 182 mil pessoas (Gressin, 2017).

A questão do "*privacy by design*" tem-se tornado no pilar para o desenho de aplicações online. Vários fornecedores de redes sociais, como Facebook, Google e o Twitter competem atualmente para providenciar um nível de privacidade nas suas aplicações que inspire confiança nos seus utilizadores. Dispor deste conceito como um modelo para o desenho de aplicações irá oferecer aos utilizadores mais autoridade para decidir que tipo de informação pretendem eles partilhar e com quem (Aldhafferi et al., 2013).

Com vista à redução das preocupações com a privacidade das pessoas e a sua potencial ameaça para o comércio eletrónico e desenvolvimento da economia digital, a Comissão

[18] Equifax – Uma das três principais agências de informação de crédito dos Estados Unidos da America.

Europeia em 2012 anunciou um projeto de reforma regulatória da Diretiva de Proteção de Dados da EU de 1995. O Regulamento Geral sobre a Proteção de Dados (RGPD) aprovado em 27 de abril de 2016 vem de forma incisiva esclarecer regras relativas à proteção dos dados pessoais de todos os cidadãos do espaço da União Europeia, concretamente em relação às redes sociais online, a Comissão Europeia propõe fortalecer a proteção da privacidade online criando e promovendo o "direito ao esquecimento", "*privacy by default*" e o "*privacy by design*". Estas novas regras pretendem permitir que os utilizadores possam eliminar informação pessoal alojada na Internet, definir padrões de alta privacidade por omissão, e considerar preocupações de privacidade na fase de desenvolvimento de *software* / aplicações (Cecere et al., 2015).

2.4. Ameaças, riscos e perigos

2.4.1. As ameaças e riscos da perda de privacidade

As gerações atuais vivem num mundo onde a comunicação é praticamente instantânea, onde uma grande quantidade de dados está instantaneamente disponível ao toque de uma tecla (ou ecrã), num ambiente tão tecnologicamente saturado e digitalmente definido, damos por certo que quase toda a informação pode ser obtida na Internet. Mas esta condescendência combinada com *chat rooms*, fóruns, *blogs*, e redes sociais online pode provar-se embaraçosa ou até mesmo perigosa (Rosenblum, 2007).

Ao mesmo tempo que a popularidade do uso de redes sociais online aumenta, também aumentam as ameaças de segurança e privacidade para os utilizadores destas redes. As redes sociais online permitem a partilha de fotos, vídeos, atividades, interesses e muitos outros aspetos da vida pessoal dos indivíduos. Contudo estas redes são também uma fonte de variadíssimas ameaças para a segurança dos seus utilizadores, em grande parte devido à quantidade e qualidade da informação que os utilizadores guardam nestas redes, tornando-se alvos muito apetecíveis tanto para *hackers*[19] como para outras pessoas que dispondo de tempo se dedicam a explorar o sistema para proveito próprio (Sadeghian et al., 2013).

[19] Hacker: [originalmente, alguém que produz mobiliário com um machado] é uma pessoa que gosta de explorar os detalhes de sistemas programáveis e de como ampliar as suas capacidades, ao contrário da maioria dos utilizadores, que preferem aprender apenas o mínimo necessário sobre os referidos sistemas. (Raymond & Steele, 1996).

A perda de privacidade inerente ao uso das redes sociais, acarreta, inevitavelmente, ameaças e riscos para os seus utilizadores. Um dos perigos mais frequente e óbvio de publicar nas redes sociais online é o caso crasso de deixar um registo digital permanente de imagens e observações compromissórias que podem ser pesquisadas e acedidas por terceiros tentando avaliar o caráter por exemplo de um candidato para um emprego, admissão escolar ou outra posição competitiva para a qual os candidatos devem ser selecionados e eliminados. A Internet é uma paisagem virtual de comunicação persistente que pode ser prejudicial para carreiras e oportunidades académicas, se vistas fora do contexto social original (Rosenblum, 2007).

Para além da falta de privacidade social temos também o uso abusivo de informação privada pelas organizações, grandes conglomerados estão a usar as redes sociais como meio publicitário, dispõem de um publico cativo, um indicador de preferências de compra, e um tipo de registo abreviado de tendências demográficas (Rosenblum, 2007). Por outro lado, muitas companhias estão envolvidas em práticas questionáveis de coleta e partilha de dados, por exemplo em 2012 a Nissan, sem informar os proprietários, reportou a localização, velocidade e direção dos seus carros do modelo "Leaf" a sites que outros utilizadores poderiam aceder através de um leitor RSS incorporado. Da mesma forma, existem relatórios que *smartphones* iPhone e Android têm enviado secretamente informações sobre a localização dos seus utilizadores para a Apple e Google (Kshetri, 2014).

Mesmo utilizadores com elevadas preocupações com privacidade e perfis exemplarmente configurados do ponto de vista de manutenção da privacidade, estão sujeitos a técnicas que permitem a utilizadores não privilegiados, através do uso de informação de grupo, prever com elevada taxa de precisão informações sensíveis (Zheleva & Getoor, 2009). Utilizando apenas registos públicos de comportamento, como por exemplo os *likes* no Facebook, é possível prever atributos altamente sensíveis da personalidade de uma pessoa, tais como: orientação sexual, etnia, visão religiosa e política, traços de personalidade, inteligência, felicidade, uso de substancias aditivas, pais separados, idade e sexo (Kosinski, Stillwell, & Graepel, 2013).

Toda a informação partilhada nas redes sociais online pode ser usada contra os utilizadores através de ataques cibernéticos (*cyber-attacks*) (Sadeghian et al., 2013). O objetivo dos ataques sociotécnicos é geralmente roubar ou dar uso de forma abusiva a informação, que supostamente não é publica, nomeadamente para fins de lucro financeiro

ou para desacreditar uma pessoa, empresa ou instituição (Nagy & Pecho, 2009). O acesso à informação sensível pode ainda despoletar riscos de terrorismo, extorsão financeira e extorsão física ou sexual (Aldhafferi et al., 2013).

2.4.2. Ataques aos utilizadores

Os *hackers* estão sempre um passo à frente dos especialistas em segurança. A sua cultura passa pela subversão e abuso de vulnerabilidades humanas para lançarem ataques de engenharia social, ao mesmo tempo que tentam enganar os utilizadores, fazendo-os crer que se tratam de ações legítimas.

Existem diferentes tipos de ameaças nas redes sociais online, são elas:

a. *Phishing*: os ataques de *phishing* normalmente passam pelo uso de réplicas falsas de sites ou emails que se fazem passar por legítimos com o intuito de conduzir as vitimas a revelaram informação privada, habitualmente conjuntos de credenciais de acesso a websites como por exemplo sistemas de *homebanking* (Sadeghian et al., 2013).

b. Endereços curtos maliciosos (*Malicious Shortened URL*): *software* malicioso (*malware*) pode ser espalhado com a ajuda de sites de redes sociais. Um exemplo disso é a disseminação de *links* para sites contendo código malicioso no *News Feed* de amigos da vítima, como forma de esconder o endereço malicioso são utilizados serviços de redução de endereços ofuscando desta forma o endereço malicioso (Sadeghian et al., 2013).

c. Roubo de identidade: partilhar informação pessoal numa rede social online pode permitir aos atacantes coletar informação suficiente para capturar a identidade da vítima. Apenas alguns detalhes pessoais simples podem providenciar informação suficiente para o atacante "adivinhar" *passwords*, respostas para mecanismos de recuperação de *password* e muito mais. Por exemplo pode ser usada informação dos gostos "*likes*" de uma pessoa no Facebook, ao gostar da página de um banco, a vitima está a providenciar informação que possivelmente a liga a essa instituição, com esta informação o atacante pode desenhar um ataque do tipo *Phishing* por forma a roubar as credenciais de acesso dessa pessoa ao sistema de *homebanking*. Outro exemplo é a colheita de informação pública como nome, país, cidade, data de

nascimento e fotografia para a construção de bases de dados que mais tarde podem ser usadas para a criação de documentos de identificação falsa (Aldhafferi et al., 2013; Sadeghian et al., 2013). Em 2009 foi tecnicamente demonstrada a possibilidade do desenvolvimento de ataques automáticos de roubo massivo de identidades em sites de redes sociais (Bilge et al., 2009).

d. Aplicações de terceiros maliciosas: alguns sistemas de redes sociais online, como por exemplo o Facebook ou o Twitter permitem a aplicações de terceiros interagirem com os dados existentes dentro do perfil dos seus utilizadores, muitas das vezes dispondo de total acesso a todo o conteúdo do perfil. Estas aplicações podem ser maliciosas de forma intencional ou serem vulneráveis de forma a serem exploradas por atacantes. Mais tarde o atacante pode dispor de todos os privilégios que a aplicação deteve, mesmo que temporariamente, sobre os dados do utilizador da rede social (Sadeghian et al., 2013).

e. *Spam*: mensagens de anúncios enviadas em massa para os utilizadores de redes sociais online. O Spam é um dos riscos de segurança nas redes sociais online, dado que a sua taxa de sucesso comparativamente com o spam tradicional propagado por e-mail é maior nas redes sociais online (Aldhafferi et al., 2013; Sadeghian et al., 2013).

f. Falsos Utilizadores: as redes sociais tentam facilitar o processo de registo de novos utilizadores, este procedimento sem complicações incentiva os utilizadores a se inscreverem mais facilmente, por outro lado, também facilita o processo de criação de contas falsas. O Facebook revelou uma estatística indicando que em 2013 aproximadamente 83 milhões dos seus utilizadores eram falsos (Sadeghian et al., 2013). Neste tipo de ataque o atacante cria uma conta falas com aspeto legítimo, nome falso, cidade, data de nascimento e algumas fotografias tudo falso. De seguida tenta conectar-se com a vítima, na maioria dos casos o atacante usa uma identidade com o sexo oposto ao da vitima, ao aceitar este pedido de amizade de uma conta falsa a vítima vai expor toda a informação pessoal protegida pela esfera de privacidade delimitada junto do atacante (Sadeghian et al., 2013).

g. Redireccionamentos de aspeto legítimo: quase todos os sites de rede sociais dispõem de páginas específicas para redirecionar os seus utilizadores para endereços externos e/ou internos. Muitas vezes os atacantes exploram estas

páginas para redirecionarem os utilizadores para endereços maliciosos, esta técnica à semelhança dos endereços curtos é muito usada para esconder e ofuscar endereços maliciosos das vítimas. Atualmente a maioria dos sites de redes sociais apresentam um aviso indicando que o utilizador está prestes a sair do site da rede social para outro site. Este tipo de alertas tem como objetivo mitigar este tipo de ataques (Sadeghian et al., 2013).

2.4.3. Integridade física em risco?

Numa esfera mais ligada à integridade física do utilizador de redes sociais, temos dois tipos de ameaças especialmente incidentes nas gerações mais novas: os Predadores Sociais e o *Cyberbulling*.

As redes sociais online já foram utilizados por predadores sexuais, perseguidores e pornógrafos para se aproximarem de menores por inúmeras vezes (Rosenblum, 2007). Um em cada seis adolescentes afirma já ter sido contactado *online* por alguém que não conhecia de uma forma que lhe incutiu medo ou desconforto (Madden et al., 2013).

As redes sociais online oferecem condições ótimas para potenciar o *Cyberbulling*, utilizadores frequentemente recebem mensagens não solicitadas de cariz obsceno, inapropriado ou até mesmo ameaçador (Rosenblum, 2007).

Cyberbulling é intimidação e assédio moral que acontece via dispositivos digitais, como *smartphones*, computadores ou *tablets*. O *cyberbulling* pode ocorrer através de SMS, texto, e aplicativos, ou on-line no *social media*, fóruns ou jogos onde pessoas podem ver, participar ou partilhar conteúdo. O *cyberbulling* inclui enviar, publicar ou compartilhar conteúdo negativo, prejudicial, falso ou malicioso sobre outra pessoa. Pode incluir a partilha de informações pessoais ou privadas sobre outra pessoa causando constrangimento ou humilhação. Em suma *cyberbulling* é assédio comunicado através de um modo *online* (Ybarra, Boyd, Korchmaros, & Oppenheim, 2012).

Uma das formas de abuso dos *cyberbullies* passa pela exposição nas redes sociais, por vezes em forma de caricatura, das imperfeições das suas vítimas, que de alguma forma não correspondem às expectativas de beleza da sociedade, a este fenómeno dá-se o nome de *body shaming*. O *body shaming* é uma grande questão social que se tem tornado num dos maiores problemas associados ao *cyberbullying* (Stacey, 2017), com uma maior incidência nos indivíduos do sexo feminino (Ringrose & Harvey, 2015).

O *Cyberbulling* e o assédio são problemas significativos de saúde dos adolescentes, pois estão associados a problemas psicossociais concorrentes, incluindo sintomatologia depressiva, problemas sociais e de comportamento e uso de substâncias aditivas (Ybarra et al., 2012).

2.5. Estudos prévios relacionados com o presente tema de investigação

Apresenta-se na Tabela 1 uma lista de trabalhos de investigação de referência relacionados com o tema da privacidade e exposição na Internet de um modo geral e em particular nas redes sociais online

Tabela 1 - Principais estudos prévios sobre privacidade e SNS

Autore(s)	Título	Objetivo do estudo
(Malhotra et al., 2004)	Iternet Users' Information Privacy Concerns (IUIPC)	Estudo pioneiro a abordar as questões de preocupações de privacidade dos utilizadores da Internet.
(Gross & Acquisti, 2005)	Information Revelation and Privacy in Online Social Networks	Dois dos principais autores sobre o estudo dos sites de redes sociais online, abordam questões de exposição e privacidade nos SNS.
(Acquisti & Gross, 2006)	Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook	De novo Gross e Acquisti estudam as preocupações com a privacidade nas redes sociais aflorando o conceito do paradoxo da privacidade.
(Barnes, 2006)	A privacy paradox: Social networking in the United States	Desenvolvimento e aplicação da construção "paradoxo da privacidade" verificado em adolescentes no Estados Unidos da América nos SNS.
(Boyd & Ellison, 2007)	Social network sites: Definition, history, and scholarship	Trabalho incontornável no ramo das redes sociais online, aparecimento da primeira definição de rede social online.
(Rosenblum, 2007)	What anyone can know: The privacy risks of social networking sites	Rosenblum explora os riscos de falta de privacidade no uso dos sites das redes sociais.
(Krasnova et al., 2009)	"It Won't Happen To Me!": Self-Disclosure in Online Social Networks	Trabalho de investigação sobre a exposição e as preocupações de privacidade dos utilizadores nos SNS.
(Boyd & Hargittai, 2010)	Facebook privacy settings: Who cares?	Estudo sobre a utilização das definições de privacidade no Facebook por jovens de 18 e 19 anos.
(Shin, 2010)	The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption	Estudo da relação de confiança, segurança e privacidade com a adoção do uso de sites de redes sociais.
(Sadeghian et al., 2013)	Security Threats in Online Social Networks	Trabalho com a identificação dos principais riscos de segurança nos SNS e sugestões de mitigação.
(Chen & Chen, 2015)	Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection	Estudo de influência de preocupações com a privacidade na gestão de privacidade nos SNS.

(Bergström, 2015)	Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses	Avaliação das preocupações com a privacidade online.
(Cecere et al., 2015)	Perceived Internet privacy concerns on social networks in Europe	Estudo da perceção de privacidade nos SNS sobre 22 mil indivíduos em 26 países da EU.
(Hargittai & Marwick, 2016)	"What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy	Estudo sobre a aplicabilidade do paradoxo da privacidade e uma crescente apatia na preocupação dos indivíduos mais jovens com a sua privacidade online.

Capítulo 3 – Apresentação da investigação

3.1.Fases da investigação e abordagem metodológica

Na revisão de literatura ficou evidente que as novas tecnologias de informação abrem novas possibilidades e desafios ao contacto interpessoal. Estes novos meios de comunicação vêm de forma irrevogável alterar o horizonte das redes sociais sobre as quais a espécie humana há muito que se baseia. A influência dos *social media* e das redes sociais online é particularmente incisiva nas gerações mais novas. Estas, tratam de uma área de estudo relativamente recente e em constante mutação, uma evidência desta mudança é o aparecimento de duas definições de rede social online no espaço de 6 anos (Boyd & Ellison, 2007; Ellison & Boyd, 2013).

A presença constante no dia-a-dia de dispositivos ligados à Internet, nomeadamente *smartphones*, *tablets*, *smartwatches*, TVs e todo o tipo de dispositivos que agilizam a relação das pessoas com as suas *personas* digitais, possibilitam a prevalência das redes sociais online como principal meio de socialização nas camadas mais jovens.

Em comparação com as gerações anteriores que usam as redes sociais online como um complemento da sua rede social *offline*, a geração Z e seguintes podem muito bem suplantar o uso das suas redes sociais *on-line* sobre as *offline*. Esta imersão no *on-line* vai certamente ser potenciada pelo uso da realidade virtual, cada vez mais massificado em produtos disponíveis já no mercado da eletrónica de consumo. O Facebook Spaces é já uma plataforma resultante do investimento da Facebook na Oculus VR.

O dinamismo da academia relativo ao *social media*, a constante evolução tecnológica, o aparecimento de novas e inovadoras redes sociais online, e a transformação nas relações sociais que a Geração Internet representa, levou esta investigação a prosseguir com uma abordagem que abarca em primeiro lugar uma dimensão qualitativa com a finalidade de consolidar os elementos recolhidos da revisão da literatura necessários para levar a cabo, numa segunda fase, a pesquisa quantitativa que este trabalho almeja.

Primeiramente foi realizado um estudo exploratório, que englobou, na realidade dois estudos complementares, um baseado em *focus group* e outro em entrevistas individuais. O *focus group* foi composto por 12 estudantes universitários a frequentar o primeiro ano de um curso de licenciatura. Relativamente às entrevistas, foram realizadas duas entrevistas com especialistas na área de redes sociais online. Quer no *focus group* quer no caso das entrevistas, os participantes foram informados de que sua participação era

voluntária e anónima, e que nenhuma informação privada ou pessoal seria coletada. Em ambos os casos, os dados recolhidos foram tratados com software de análise de conteúdo online – usando a plataforma Leximancer.

O planeamento baseou-se em levantar vários temas e ver como diferentes conceitos são abordados e relacionados entre si. Os dados coletados a partir das respostas foram analisados na plataforma Leximancer. Trata-se de um software de *text minning* usado para extrair conceitos significativos de conteúdo textual não estruturado. O Leximancer digere o texto por forma a encontrar conceitos possíveis, em diversas iterações são removidos todos os conceitos não significativos para o contexto. No final são produzidos gráficos que interligam os conceitos significativos encontrados.

A escolha do *focus group* como um dos instrumentos para este trabalho mostrou ser a melhor abordagem para criação de conceitos, geralmente evasivos em questionários regulares (Kitzinger, 1994). O *focus group* foi realizado por meio de entrevista semiestruturada. As entrevistas foram realizadas por meio de um guião pré-determinado.

A análise da informação recolhida na fase exploratória, composta pelo *focus group* e pelas entrevistas, forneceu conceitos fundamentais que contribuíram para construir e desenvolver um questionário, que por sua vez serviu de instrumento base para a segunda fase deste trabalho. A segunda fase englobou um estudo inferencial e correlacional, mais quantitativo. Este estudo teve como instrumento de recolha de dados um questionário *online*, desenvolvido com base não só o levantamento teórico-conceptual, mas principalmente, os conceitos e indicadores resultantes do estudo exploratório.

A distribuição do questionário foi efetuada por meio de partilha nas redes sociais, em concreto no Facebook, LinkedIn e Instagram. No caso particular do Facebook o questionário foi também partilhado em grupos fechados da comunidade académica do ISCTE-IUL. Para além da distribuição direta por via eletrónica, o questionário foi também encaminhado, com um pedido de divulgação, para praticamente a totalidade dos gabinetes de comunicação de instituições de ensino superior em Portugal e, por último, foram também efetuados pedidos de divulgação junto dos secretariados escolares das diversas escolas do ISCTE.

Os dados recolhidos no questionário foram alvo de normalização, validação e identificação e remoção de respostas erradas (por exemplo alunos com 99 anos e inscritos

em cursos com nomes sem significado), em seguida os dados foram alvo de tratamento estatístico descritivo, fatorial e correlacional.

3.2. Questão de investigação e objetivos

Nesta investigação partimos de uma questão primordial: 'Qual a importância que os estudantes universitários atribuem à privacidade e à segurança ao utilizarem as redes sociais online'. Na procura de respostas a esta grande questão, foram sistematizados sete componentes essenciais:

- A perceção da privacidade;
- A perceção de segurança;
- A relação de confiança com os serviços de redes sociais;
- A consciência (de práticas de privacidade);
- O reconhecimento de coleta de dados;
- A identificação de uso secundário não autorizado;
- A perceção de riscos.

Da revisão de literatura, consubstanciada pelos conceitos identificados no *focus group*, em conjunto com os componentes essenciais, deduzimos os objetivos que dirigem esta investigação:

- Averiguar a perceção dos estudantes universitários acerca da sua privacidade online;
- Averiguar a perceção dos estudantes universitários acerca da sua segurança em termos da informação partilhada online;
- Identificar as redes sociais usadas;
- Determinar os comportamentos típicos nas redes socias;
- Verificar a importância das redes sociais na vida pessoal, académica e profissional;
- Relacionar as dimensões encontradas sobre a segurança e a privacidade, com os comportamentos típicos nas redes sociais.

Na Figura 5 pode ver-se um diagrama dos objetivos desta investigação e as suas ligações com os diversos estudos conduzidos.

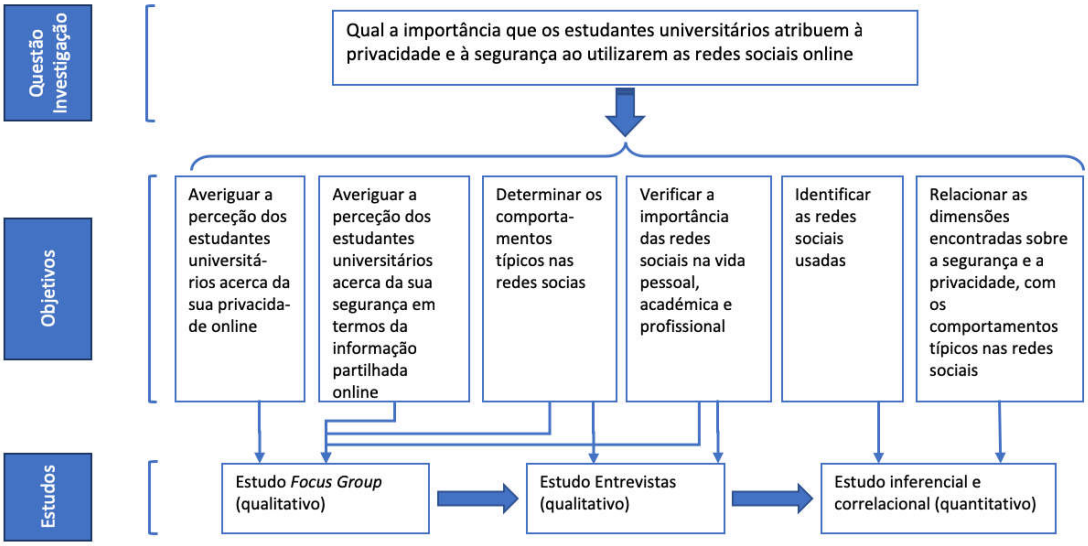

Figura 5 – Diagrama objetivos e estudos

Capítulo 4 – Fase Exploratória

4.1. Focus Group

Os *focus group* têm sido utilizados com grande sucesso nas áreas de marketing, e têm ganho grande importância em áreas como a educação, saúde, gestão, apoio à decisão e em sistemas de informação, entre outras (Freitas, Oliveira, Jenkins, & Popjoy, 1998). Consistem em grupos de discussão organizados de forma a explorar um conjunto pré-determinado de assuntos, habitualmente assentes sobre as visões e experiências das pessoas sobre as questões expostas, permitindo desta forma recolher informação de várias pessoas em simultâneo (Kitzinger, 1994). Esta técnica é especialmente útil para explorar o conhecimento e as experiências das pessoas, permitindo ao mesmo tempo saber não só o que as pessoas pensam sobre um determinado assunto, mas também, como pensam e porque pensam dessa forma (Kitzinger, 1995), permitindo desta forma alcançar as perceções das pessoas envolvidas no grupo, encorajando a participação de todos, mesmo dos elementos mais relutantes, ou das pessoas que acham que não têm mais nada a acrescentar.

Os *focus group* foram originalmente concebidos para ser usados em estudos sobre comunicação, por forma a recolher e compilar os efeitos que programas de rádio e televisão, filmes e propaganda de guerra teriam sobre a população (Kitzinger, 1994). Desta forma a aplicação desta técnica neste trabalho é na realidade um regresso às origens, isto é, este estudo visa identificar a perceção que pessoas (estudantes universitários) têm sobre um novo meio de comunicação a Internet e os *social media*.

4.1.1 Amostra

O *focus group* foi organizado nas instalações do ISCTE-IUL, com 12 alunos (N=12) do primeiro ano de licenciatura dos cursos de Gestão e Economia da ISCTE Business School. A distribuição dos elementos foi de 2 do sexo masculino e 10 do sexo feminino, com intervalo de idades compreendido entre os 19 e os 26 anos.

4.1.2 Guião de discussão e Procedimento

O *focus group* decorreu num ambiente calmo e sereno dentro de uma sala de aula reservada para o efeito, tendo durado aproximadamente uma hora. A conversa com os alunos foi conduzida de acordo com um guião de questões (apêndice A), onde após a

exposição de cada questão foi motivada a discussão entre todos os elementos de cada um dos itens explorados. Toda a iteração do grupo foi gravada em suporte de áudio a partir do qual mais tarde foi feita a sua transcrição para formato de texto.

4.1.3 Técnicas de Análise de Dados

Os textos recolhidos nas diversas questões do guião do *focus group* foram agrupados nos sete componentes essenciais do estudo; privacidade, segurança, controlo, consciencialização, recolha, uso secundário e riscos.

Com os textos agrupados foram desenvolvidas análises do texto não estruturado na ferramenta online Leximancer, nesta plataforma procedeu-se à identificação dos principais conceitos e suas interligações agrupados por cada um dos componentes essenciais e uma oitava análise que levou em conta todo o texto recolhido no *focus group*. Este processo de análise foi feito em várias interações com vista a afinar os conceitos identificados, removendo eventuais conceitos mal identificados ou não relevantes para o estudo. No final foram produzidos gráficos para cada um dos componentes essenciais do estudo (Apêndice C) e um gráfico adicional que incorpora todo o texto compilado no *focus group*, estes gráficos compreendem a identidade e interligação de todos os conceitos identificados. Dado o caráter global e agregador do oitavo gráfico, apenas este foi alvo de uma aprofundada interpretação.

4.1.4 Resultados

O estudo relativo ao *focus group*, cujos resultados são aqui apresentados, foi desenvolvido e divulgado numa publicação indexada, na conferência ICERI 2018 (11ª Conferência Internacional anual de Educação, Pesquisa e Inovação) organizada pelo *International Academy of Technology, Education and Development* (IATED). Os resultados deste estudo serão publicados no "ICERI2018 Proceedings" com o título "Remember when, on the Internet, nobody knew who you were?" (Rodrigues & Oliveira, 2018).

No gráfico a seguir (Figura 6), podemos ver todo o domínio de conceitos que emergem do *focus group*. Através da interpretação dos dados obtidos e da exploração dos conceitos representados, chegamos a alguns resultados.

Os utilizadores recorrem às redes sociais porque elas existem e sabem que isso tem um certo significado para eles como utilizadores, eles conhecem o tipo de redes sociais que existem e sabem o que está associado a elas, eles têm essa noção. Isto implica que se eles sabem o que é e têm uma noção do que são redes sociais, já sabemos porque vão lá, vão para: falar, publicitar, participar em eventos, grupos e chats, fazer comentários, rir, chorar. Em suma, divulgar o que devem e não devem (Acquisti & Gross, 2006; Boyd, 2008; Ellison & Boyd, 2013; Hallam & Zanella, 2017; Marwick & Boyd, 2014).

O conceito "utilizadores" tem uma interseção com as redes sociais, enquanto que o conceito de empresas não, isto pode significar que os utilizadores estão "dentro" das redes sociais, então mais próximos das redes sociais, no extremo poderá dizer-se que os utilizadores são as redes sociais, assim, assiste-se a uma fusão entre a vida social e a vida digital dos utilizadores (Ellison et al., 2007; Rosenblum, 2007). Resumidamente, os utilizadores sabem o que são redes sociais, mas aderem de qualquer forma.

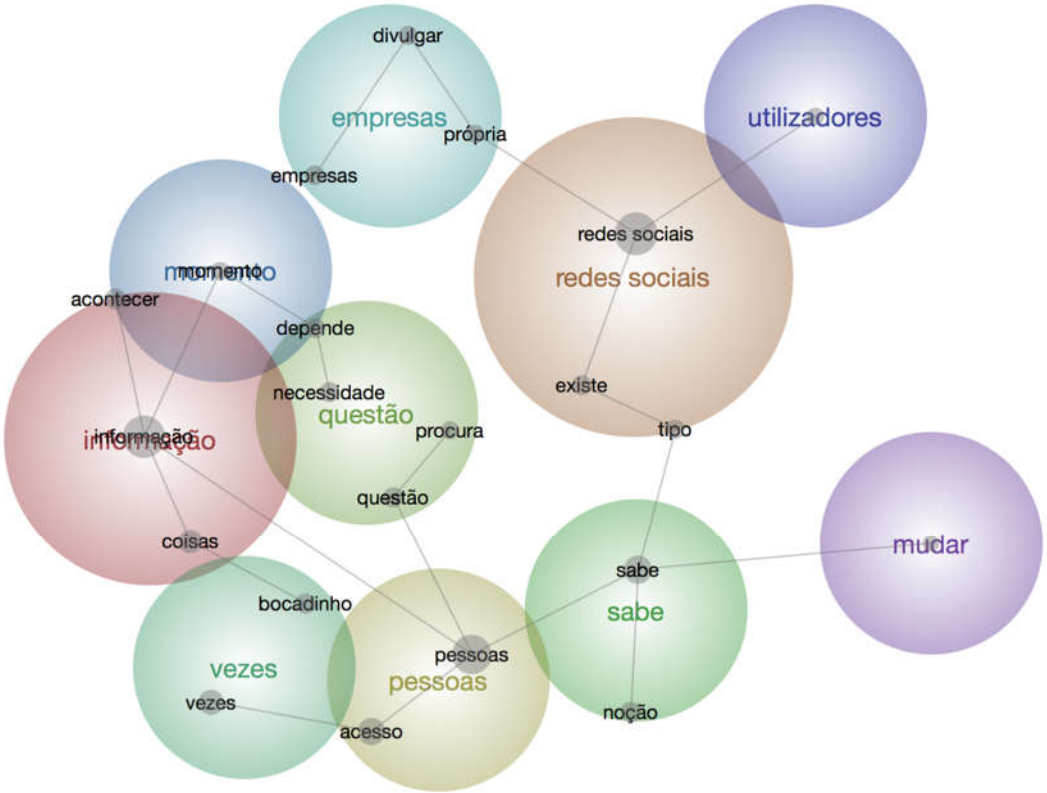

Figura 6 - Análise / Perceção de privacidade, autoexposição em redes sociais de estudantes universitários

Por outro lado, as empresas usam as redes sociais para divulgar a suas próprias iniciativas, sempre em seu próprio interesse. O conceito de "empresas" não se interliga com as redes sociais, existe uma separação, as empresas só usam as redes sociais, não fazem parte delas. Observe-se que os utilizadores também não estão ligados a mais nada

para além das redes sociais, então o conceito de redes sociais é o que interliga os utilizadores às empresas, que assim conseguem captar a atenção dos utilizadores. Do ponto de vista dos utilizadores, é o habitual, afirmam que não divulgam informação pessoal, mas efetivamente essa informação está amplamente disponível (Krasnova et al., 2009; Norberg et al., 2007).

As pessoas sabem o que são redes sociais e têm uma noção sobre isso, porém, ao mesmo tempo, existe aqui uma noção de mudança, ou seja, estamos perante uma possível mudança na noção (perceção) do que é uma rede social, assiste-se a um processo de mudança externa. De notar que esta mudança não ocorre nos utilizadores das redes sociais, mas sim nas pessoas, o que evidencia uma dissociação latente entre o utilizador e a pessoa.

Do ponto de vista das pessoas, vemos que por vezes elas acedem às redes sociais e, em parte, vão lá para procurar informação. As pessoas procuram as redes sociais basicamente para pesquisa, procurar questões, procurar informação, mas apenas às vezes, o resto do tempo as pessoas produzem informação, composta por texto, imagens, vídeo, informação de localização, etc... Por um lado, as pessoas sabem que podem mudar e eventualmente podem de algum modo também cultivar a sua privacidade, mas por outro, utilizam as redes sociais para troca de informação. Estamos aqui perante um paradoxo (Barnes, 2006), até que ponto têm as pessoas noção que ao trocar tanta informação sabem mesmo que podem mudar. Será que realmente sabem que podem mudar as questões da sua privacidade, seu comportamento e a maneira como reagem? De certa forma é uma espécie de desistência, quase como que um sentimento de apatia em relação à privacidade (Boyd & Hargittai, 2010; Hargittai & Marwick, 2016).

Outro conceito emerge, interagir nas redes sociais é uma questão do momento, as pessoas podem fazer algo num momento específico no tempo, mas partilhar algo naquele momento em particular pode deixar a pessoa a pensar nas consequências que a partilha terá no futuro. Existe a ideia que o que é vivido no momento já passou e que de certa forma já pertence ao passado, o problema é que não passa, fica gravado nas redes sociais para referência futura, e será lembrado, eventualmente fora do contexto inicial (Rosenblum, 2007). Este momento depende da necessidade de procurar por questões, que podem ser afetivas ou sociais, e como vemos uma ligação entre questões e informações, fundamentalmente as pessoas estão a partilhar e a procurar tudo o que te a ver com a sua vida pessoal (Boyd, 2014; Madden et al., 2013).

No gráfico não encontramos conceitos de privacidade, contudo é bastante relevante o foco atribuído ao conceito de informação (2ª maior dimensão) é porque de facto os alunos podem até pensar que a privacidade é uma coisa importante, mas uma vez que entram nas redes sociais esquecem-se disso.

As empresas estão entre as redes sociais e o momento, ou seja, as empresas claramente aproveitam o momento, percebem o grande papel das redes sociais que as ajuda a divulgar aquilo que fazem, assumem aqui um papel comercial, aproveitando os momentos que as pessoas vivem para exibir o que fazem e ao mesmo tempo ter acesso às informações que os utilizadores colocam nas redes sociais.

É curioso que quando a pessoa se coloca no papel do utilizador o seu comportamento muda, "uma coisa é o que eu faço como utilizador, outra coisa é o que as pessoas fazem". As pessoas em geral vivem os momentos, procuram várias questões, partilham informação, mas sabem o que são redes sociais, percebem que sabem que a qualquer momento podem mudar. Esta dicotomia utilizador / pessoa é como se o utilizador e a pessoa fossem coisas diferentes, isto é, a atitude de privacidade e o comportamento de privacidade são duas coisas diferentes (Kokolakis, 2017). Esta dicotomia é reforçada pela noção do momento presente, os alunos tendem a superestimar o benefício imediato de partilhar informação contra a eventual perda futura de privacidade (Hallam & Zanella, 2017).

4.2.Entrevistas

Além do *focus group* foram também efetuadas duas entrevistas com especialistas no campo das redes sociais e do *social media*. Estas entrevistas visaram a criação de mapas conceptuais baseados no mesmo guião de questões usado no *focus group*, permitindo desta forma ter uma visão complementar sobre os conceitos emergentes do *focus group*.

As entrevistas assim como o *focus group* são dois mecanismos disponíveis para procedermos com a fase qualitativa que este trabalho contempla. Uma das principais vantagens que a pesquisa qualitativa nos disponibiliza é a capacidade de examinar os efeitos contextuais, o estudo qualitativo pode demonstrar a sensibilidade ao contexto, evidenciando a consciência das perspetivas dos participantes (Yardley, 2017). É exatamente esta sensibilidade contextual que foi procurada ao entrevistar professores especialistas na área das redes sociais.

4.2.1 Amostra

Foram realizadas duas entrevistas com professores do ISCTE-IUL com demonstrado currículo na área das redes sociais e dos sistemas de informação, ambos os professores fazem parte da Escola de Tecnologias e Arquitetura (ISTA).

4.2.2 Guião de discussão e Procedimento

As entrevistas foram individuais, tendo durado aproximadamente uma hora, e obedecido ao mesmo guião de questões (apêndice B), sendo dada total liberdade ao entrevistado para explorar cada um dos temas abordados. Todas as entrevistas foram gravadas em suporte de áudio, tendo sido feita depois a transcrição para formato de texto.

4.2.3 Técnicas de Análise de Dados

O texto recolhido nas diversas questões do guião do *focus group* foram agrupados em nove componentes essenciais; privacidade, segurança, confiança, atitude perante redes sociais, controlo, consciencialização, recolha, uso secundário e riscos. Com os textos agrupados foram feitas análises do texto não estruturado na ferramenta online Leximancer, nesta plataforma procedeu-se à identificação dos principais conceitos e suas interligações agrupados por cada um dos componentes essenciais e uma décima análise que levou em conta todo o texto recolhido nas duas entrevistas. Este processo de análise foi feito em várias interações com vista a afinar os conceitos identificados, removendo eventuais conceitos mal identificados ou não relevantes para o estudo. No final foram produzidos gráficos para cada um dos componentes do estudo (Apêndice C) e um gráfico adicional que incorpora todo o texto compilado nas entrevistas, estes gráficos compreendem a identificação e interligação de todos os conceitos identificados.

4.2.4 Resultados

Apesar das questões nas entrevistas serem praticamente as mesmas usadas no guião do *focus group*, podemos ver no gráfico gerado da análise das entrevistas (Figura 7) um novo conjunto de conceitos extraídos das entrevistas com os especialistas. Da análise aos conceitos sintetizados chegamos a alguns resultados.

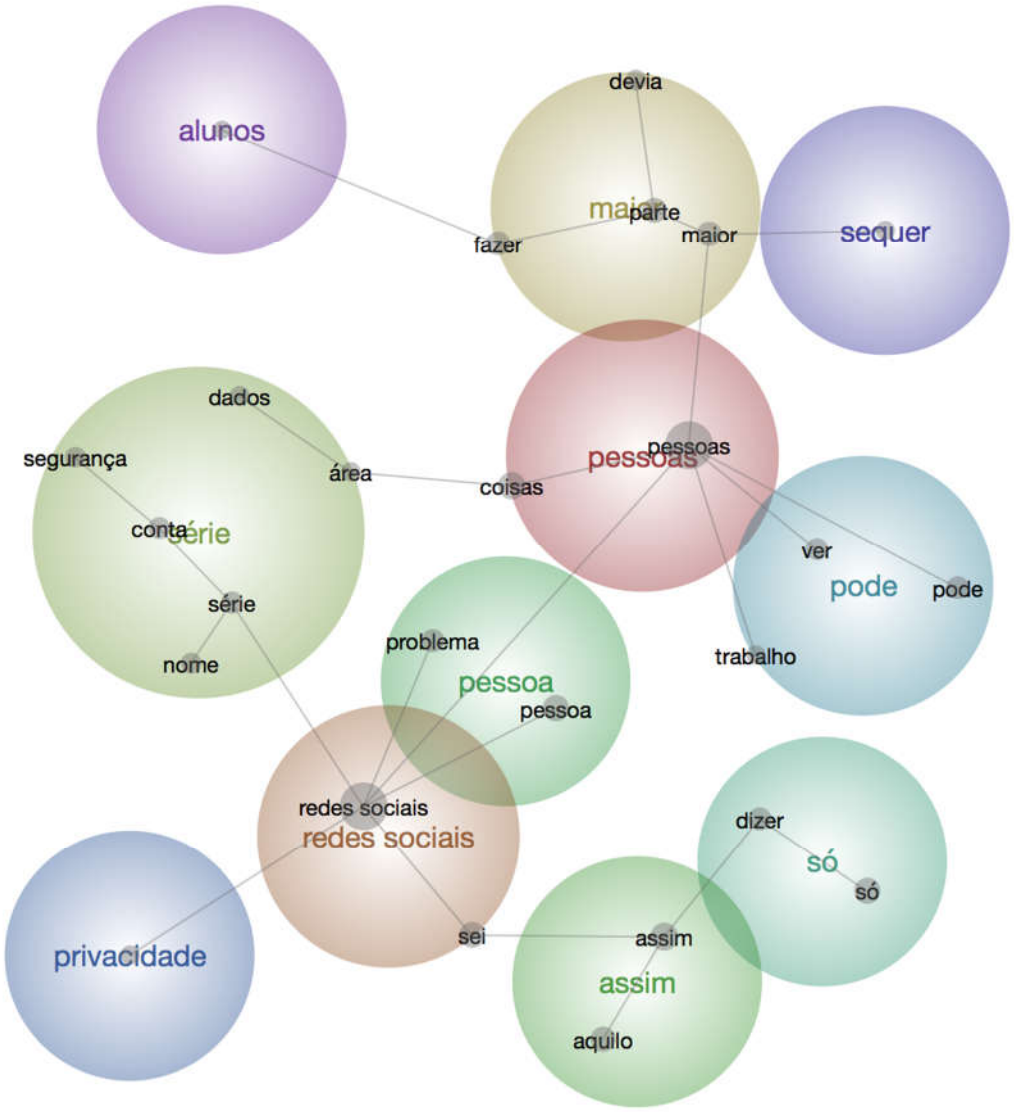

Figura 7 - Análise / Perceção de privacidade, autoexposição em redes sociais de professores universitários

Mais uma vez vemos uma interseção entre redes sociais e as pessoas, reforçando a ideia de que as pessoas são as redes sociais, potenciando a mistura entre a vida social e a vida digital das pessoas (Ellison et al., 2007; Rosenblum, 2007).

A privacidade nas redes sociais só é possível se forem observados diversos cuidados com a divulgação de dados e com a manutenção da segurança desses mesmos dados, as pessoas não devem contar tudo, infelizmente este comportamento ainda não é seguido pela maior parte das pessoas (Hallam & Zanella, 2017).

O problema da falta de privacidade nas redes sociais ocorre da partilha de todo o tipo de coisas por parte das pessoas. Por sua vez esta partilha excessiva de informação conduz

à redução de privacidade, que em muitos casos pode por em causa a situação laboral das pessoas, ou as futuras pretensões de vir a ter um trabalho (Rosenblum, 2007).

É este risco para a atividade profissional que a partilha de dados nas redes sociais acarreta que os atuais alunos do ensino superior, na sua maioria, nem sequer imaginam ou fazem ideia, e que, apesar de tudo, já deviam preocupar-se com esta problemática.

Os alunos, assim como a maior parte das pessoas têm uma baixa consciência do que pode acontecer com a informação partilhada nas redes sociais (Nagy & Pecho, 2009), bem como com o uso e destino que esta informação poderá ter (Krishnamurthy & Wills, 2008). É toda esta serie de dados pessoais e privados, começando em muitos casos pelo próprio nome, que são partilhados nas redes sociais muitas vezes de forma pública (Gross & Acquisti, 2005) e que têm de ser geridos de forma mais criteriosa, só assim os conceitos de privacidade e redes sociais poderão coexistir (Young & Quan-Haase, 2013).

Nesta análise surge o conceito "aluno" separado do conceito de pessoas, observa-se aqui um reforço da ideia de mudança já patente no *focus group*, de certa forma verifica-se que as pessoas de uma forma geral apresentam comportamentos de risco que já só uma parte dos alunos reproduz, a cultura tecnológica começa a interiorizar-se nas novas gerações.

Capítulo 5 – Fase inferencial e correlacional

5.1.Amostra e população

Na etapa quantitativa deste trabalho foram recolhidos dados por intermédio de um questionário eletrónico, distribuído a estudantes de diferentes ciclos no ensino superior, em Universidades e Institutos Superiores em Portugal. A amostra foi constituída por 258 participantes de ambos os géneros com idades compreendidas entre os 17 e os 61 anos.

Relativamente ao género, 66,3% eram do sexo feminino (N = 171) e 33,7% eram do sexo masculino (N = 87). Em relação à idade, 43,4% tinham até 20 anos de idade (N = 112), 33,3% tinham entre 21 e 25 anos de idade (N = 86), 12,8% entre 26 e 30 anos de idade (N = 33), os restantes 10,5% tinham mais de 30 anos de idade (N = 27). Relativamente ao tipo de curso a frequentar, 46,5% dos inquiridos eram alunos de Licenciatura (N = 120), a frequentar Mestrado eram 45,7% indivíduos (N = 118), alunos de Doutoramento responderam 4,3% (N = 11) e por fim alunos a frequentar outros tipos de cursos responderam 3,1% (N = 8).

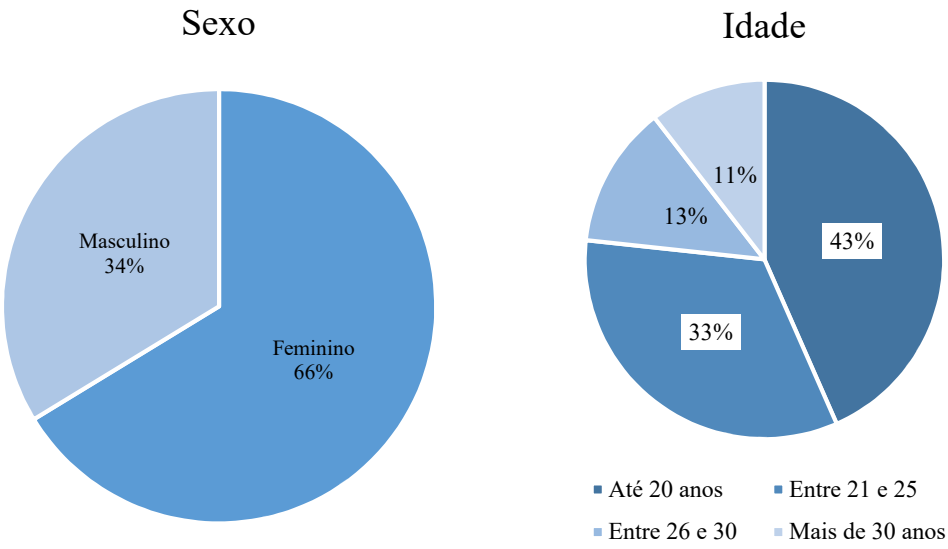

Figura 8 - Distribuição inquiridos por género e idade

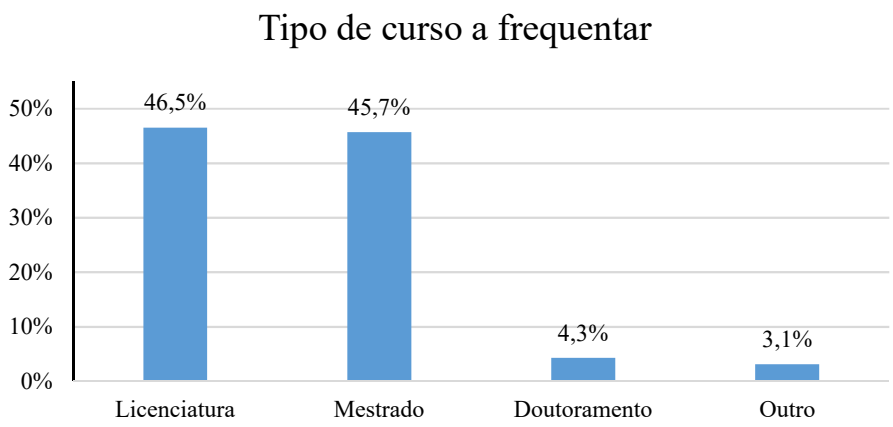

Figura 9 - Distribuição de alunos por tipo de curso a frequentar

Dos alunos a frequentar uma Licenciatura, 38,3% (N = 46) estavam no 1º ano, 28,3% (N = 34) estavam no 2º ano, 23,3% (N = 28) estavam no 3º ano e 10,0% (N = 12) indicaram estar em anos superiores ao 3º. Dos alunos em Mestrado, 41,5% (N = 49) estavam no 1º ano, 27,1% (N = 32) estavam no 2º ano, 7,6% (N = 9) no 3º ano e 23,7% (N = 28) disseram estar no 4º ou 5º anos. Grosso modo 40,1% (N = 103) dos alunos que responderam ao questionário estavam a frequentar o 1º ano, 27,2% (N = 70) a frequentar o 2º ano, 16,3% (N = 42) no 3º ano e 16,3% (N = 42) no 4º e 5º anos.

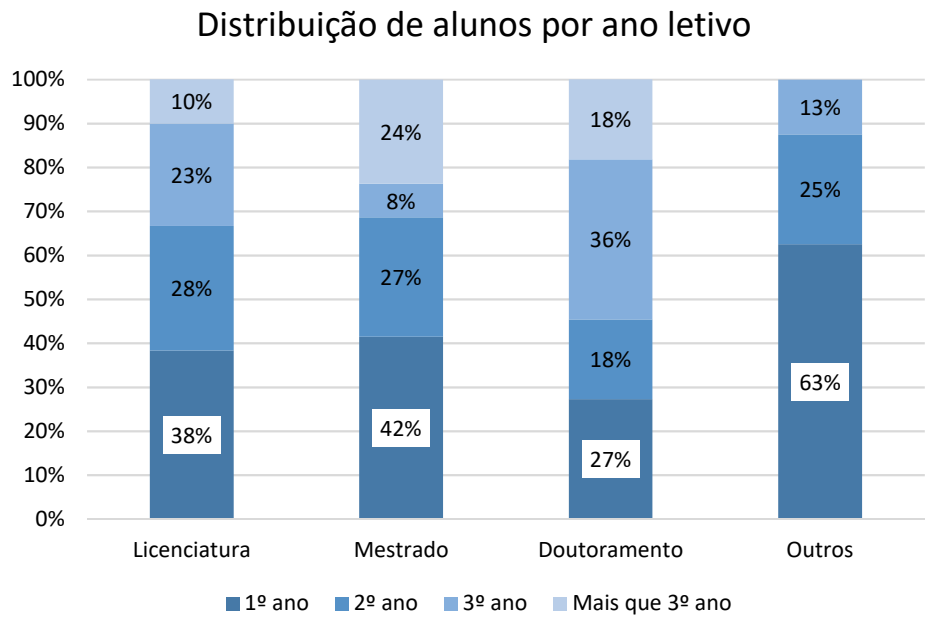

Figura 10 - Distribuição de alunos por ano letivo

Dos alunos inquiridos 21,3% (N = 55) frequentavam o ISCTE-IUL, 23,3% (N = 60) frequentavam a Universidade de Aveiro, 22,5% (N = 58) frequentavam a Universidade

de Lisboa, 14,7% (N = 38) a Universidade Nova de Lisboa e 18,2% (N = 47) distribuem-se por outras 24 instituições de ensino superior em Portugal (cf. Apêndice E).

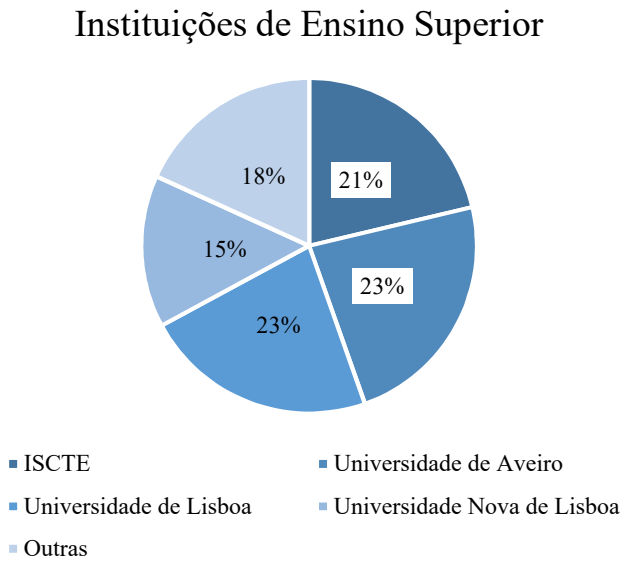

Figura 11 - Distribuição de alunos por instituições de ensino superior

De todos os respondentes, 51,9% estudavam no mesmo concelho onde residiam antes de frequentar o curso (N = 134), 48,1% dos alunos estudavam num concelho diferente do concelho de onde são oriundos (N = 124), isto é, quase metade da amostra representa alunos deslocados da sua morada habitual.

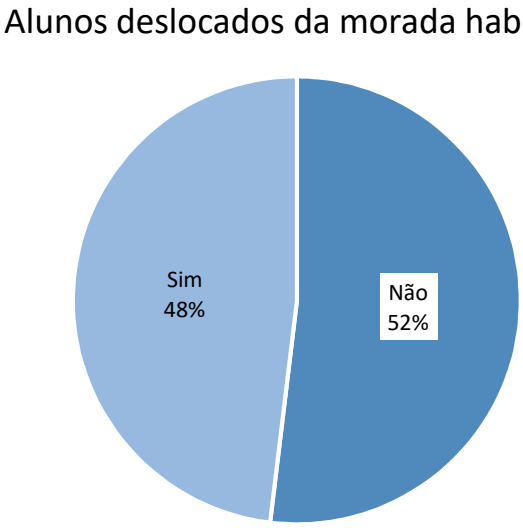

Figura 12 - Distribuição de alunos deslocados da morada habitual

5.2.Questionário

Partindo da revisão de literatura e dos resultados obtidos na fase exploratória (no *focus group* e nas entrevistas), foi elaborado um questionário (cf. Apêndice D). Apesar da possibilidade de uma baixa obtenção de respostas e/ou respostas não válidas, associada geralmente a esta técnica de recolha de dados, derivada entre outros fatores da associação deste tipo de recolha de dados a abordagens de venda ou comerciais (Krosnick, 1999), a escolha desta técnica neste trabalho teve como principal ponderador a possibilidade de uma rápida obtenção de respostas (em virtude da janela temporal deste trabalho) e de um menor risco de distorção. Em virtude de a população em estudo serem estudantes universitários, estamos perante indivíduos que pelo facto de participarem frequentemente em sondagens e questionários dispõem de uma menor resistência à participação em questionários (Krosnick, 1999).

O questionário encontra-se dividido em duas partes, uma primeira parte referente à caraterização sociodemográfica do respondente e uma segunda parte relacionada com o âmago desta investigação. Na segunda parte do questionário foram feitas perguntas – associadas a escalas do tipo *Likert*, entre 1 e 5: onde por exemplo, o valor inferior pode corresponder a 1 (Nunca) e o valor superior a 5 (Muito frequentemente) – relativas à utilização de redes sociais, privacidade nas redes sociais, segurança nas redes sociais, tipo de utilização das redes sociais, importância das redes sociais e exposição nas redes sociais (cf. Apêndice D).

O questionário foi produzido na plataforma Qualtrics e distribuído nas redes sociais LinkedIn, Facebook e Instagram, por email junto da comunidade docente do ISCTE-IUL, por email junto dos departamentos de comunicação das principais instituições de ensino superior em Portugal e via email junto das secretarias escolares do ISCTE.

5.3.Técnicas de Análise de Dados

Uma vez recolhidos os dados, foi desenvolvido o seu tratamento na ferramenta IBM SPSS Statistics v.24 para macOS. Numa primeira instância, recorreu-se à estatística descritiva para a caraterização da amostra e de todas as questões do questionário. Numa segunda interação, levou-se a cabo a realização de cinco análises de componentes principais para alcançar as dimensões relacionadas com a importância que os estudantes universitários atribuem à privacidade e segurança ao utilizarem as redes sociais online.

Foram também desenvolvidas análises correlativas entre as variáveis que constituem cada dimensão encontrada nas esferas da privacidade, segurança e tipo de utilização das redes sociais.

5.4. Resultados

Com vista a responder ao primeiro objetivo, *averiguar a perceção dos estudantes universitários acerca da sua privacidade online*, foram utilizados os dados recolhidos na pergunta 2 da parte II do questionário (cf. Apêndice D). Nesta pergunta os alunos classificaram em função da sua importância, com uma escala de 1 (nada importante) a 5 (muito importante), uma série de afirmações relativas à privacidade nas redes sociais. Com exceção da questão relacionada com a publicidade direcionada para o utilizador (M = 3,24) – publicidade esta que recorre a técnicas de *tracking*, também elas invasivas do ponto de vista de privacidade – a maioria dos participantes demonstrou achar muito importante grande parte das afirmações, destacando-se elementos como, a capacidade de controlar e gerir o nível de privacidade na rede social (M = 4,77), ter conhecimento de como a informação pessoal será usada pela rede social (M = 4,72), poder gerir que organizações externas poderão ter acesso à informação privada (M = 4,72) e dispor de mecanismos eficazes para resolver situações de violação de privacidade (M = 4,72).

Com o intuito de averiguar a perceção relativa à privacidade *online*, realizou-se uma análise fatorial de componentes principais (ACP) com os itens da questão 2. Esta ACP permitiu-nos identificar as dimensões centrais na perceção dos estudantes acerca da sua privacidade online (Tabela 2). Foram identificados dois fatores, que correspondem às dimensões, compreendidas na perceção de privacidade online.

O primeiro fator (41,47% de variância total explicada, com alfa de Cronbach α = 0,747) agrupa os itens referentes à privacidade providenciada pela rede social.

O segundo fator (15,05% de variância total explicada, com alfa de Cronbach α = 0,675) agrupa os itens referentes à capacidade de exercer controlo sobre a informação privada na rede social.

Tabela 2 - Estrutura fatorial das dimensões associadas à perceção da privacidade online

	Componentes	
	Privacidade da rede social	**Capacidade Controlo**
Dispor de processos eficazes para resolver situações de violação de privacidade	,888	,085
A rede social ter uma política de privacidade clara, simples e de fácil compreensão	,862	,104
Saber como é que as minhas informações pessoais serão usadas	,626	,397
Não divulgar a minha localização, quer por intermédio de mensagens, quer por fotografias ou vídeos	,515	,305
Remover a permissão de acesso à informação de localização às "Apps" de redes sociais	,089	,728
Não fornecer informação privada/pessoal nas redes sociais	,217	,695
Poder contar com a rede social para proteger a minha privacidade	,115	,685
Poder gerir que (outras) entidades/organizações podem aceder a informações sobre mim	,288	,659
Valores próprios	3,31	1,20
Variância Explicada (%)	41,47	15,05
Percentagem Acumulada	41,47	56,53
Alfa de Cronbach (α)	0,747	0,675

Nota: Resultado da ACP: matriz após rotação varimax, com normalização Kaiser, convergente em 3 iterações. Medida KMO = 0,772, Teste de Bartlett = 524,065, Significância = 0,000

Para o segundo objetivo deste trabalho, *averiguar a perceção dos estudantes universitários acerca da sua segurança em termos da informação partilhada online*, foram utilizados os dados recolhidos na pergunta 3 da parte II do questionário (cf. Apêndice D). Nesta questão foi pedido aos alunos para classificar em função da sua importância, um conjunto de frases relacionadas com a segurança nas redes sociais, novamente foi usada uma escala de 1 (nada importante) a 5 (muito importante). A maioria dos alunos consideraram todas as afirmações como muito importantes, das afirmações que recolheram maior adesão no nível de muito importante realçam-se itens como, ter a garantia que pessoas não autorizadas não tenham acesso às informações pessoais (M = 4,79), ter a garantia que a informação colocada na rede social não pode ser alterada por terceiros (M = 4,77), dispor de mecanismos ativos de mitigação de roubo de identidade (M = 4,69) e a rede social dispor de um elevado nível de privacidade (M = 4,69).

Por forma a aferir a perceção em relação à segurança online, foi efetuado uma análise fatorial de componentes principais (ACP) com os itens da questão 3. Esta ACP permitiu-nos identificar as dimensões na perceção dos estudantes acerca da sua segurança online (Tabela 3). Foram identificados três fatores, que correspondem às dimensões, compreendidas na perceção de segurança online.

O primeiro fator (42,98% de variância total explicada, com alfa de Cronbach α = 0,802) agrupa os itens referentes ao conhecimento de quem pode aceder à informação privada.

O segundo fator (7,95% de variância total explicada, com alfa de Cronbach $\alpha = 0,742$) representa os itens referentes à segurança da informação arquivada na rede social.

O terceiro fator (7,53% de variância total explicada, com alfa de Cronbach $\alpha = 0,736$) reúne os itens que dizem respeito a mecanismos de proteção reforçados na rede social.

Tabela 3 - Estrutura fatorial das dimensões associadas à perceção da segurança online

	Componente		
	Conhecimento	**Segurança**	**Proteção**
Poder autorizar explicitamente que organizações podem aceder aos meus dados	,822	,089	,022
Poder definir para cada entidade/organização, quais os dados/informações a que permito o acesso	,749	,196	,185
Não partilhar informações que poderão vir a ser usadas de formas que não prevejo	,654	,131	,391
Conhecer a honestidade das redes sociais relativamente ao uso que fazem da informação dada pelos utilizadores	,564	,354	,310
Dispor de mecanismos ativos para mitigar o roubo de identidade	,541	,398	,207
A rede social ter (por defeito) as funcionalidades que usam a localização desligadas ou desativadas	,059	,721	-,063
Ter a garantia de que pessoas não autorizadas não tenham acesso às minhas informações pessoais	,188	,715	,308
Ter a garantia de que a informação fornecida à rede social não pode ser alterada por terceiros	,300	,583	,325
Saber que toda a informação fornecida à rede social está segura (de outros utilizadores ou agentes exteriores)	,445	,545	,345
Saber que a minha informação só pode ser acedida por mim (por exemplo, usando mecanismos de encriptação)	,399	,498	,145

	Componente		
	Conhecimento	**Segurança**	**Proteção**
A rede social deve oferecer mecanismos de autenticação reforçados (por exemplo: autenticação a 2 fatores (password + código), autenticação com certificados pessoais, obrigatoriedade de usar passwords muito complexas, etc.)	,176	-,065	,805
A rede social garantir um elevado nível de segurança	,197	,298	,796
A rede social possibilitar um elevado nível de privacidade	,139	,408	,555
Ao usar uma rede social ter o cuidado de não revelar informação pessoal ou confidencial	,345	,428	,503
Valores próprios	6,01	1,11	1,05
Variância Explicada (%)	42,98	7,95	7,53
Percentagem Acumulada	42,98	50,94	58,47
Alfa de Cronbach (α)	0,802	0,742	0,736

Nota: Resultado da ACP: matriz após rotação varimax, com normalização Kaiser, convergente em 4 iterações.
Medida KMO = 0,886, Teste de Bartlett = 1245,298, Significância = 0,000

O terceiro objetivo deste trabalho pretende *identificar as redes sociais usadas pelos estudantes*, para responder a este objetivo foram usadas as respostas à pergunta 1 da Parte II do questionário (cf. Apêndice D). Esta questão era composta por uma lista de redes sociais online onde para cada uma delas foi pedido aos alunos que indicassem a frequência de utilização, foi usada uma escala de 1 (nunca) a 5 (muito frequentemente). Os critérios de escolha das redes sociais a constar nesta lista foram: rede dispor de pelo menos vinte milhões (20.000.000) de utilizadores registados[20], ser um sistema ativo e disponível em Portugal, ser uma rede social aberta (qualquer individuo pode aderir) e não ser uma rede social de cariz exclusivamente sexual ou apenas para promover encontros (*dating*).

Da análise dos dados recolhidos na pergunta 1, verificamos que cinco redes sociais se destacam das restantes na frequência da sua utilização, Facebook Messenger (M = 4,44), YouTube (M = 4,34), Facebook (M = 4,15), Instagram (M = 3,92) e WhatsApp (M = 3,56) são as redes sociais mais usadas pelos inquiridos (Figura 13). As redes sociais Skype (M = 2,39) e LinkedIn (M = 2,16) apesar de serem utilizadas registam valores bastante modestos. As restantes redes sociais têm uma expressão de utilização praticamente nula.

[20] Statista - The Statistics Portal (2018, Julho). Lista de sites de redes sociais mundialmente mais populares em função do número de utilizadores. Retirado de https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users2

O facto de 40,1% dos alunos que responderam ao questionário estarem no 1º ano do curso pode explicar a baixa utilização da rede LinkedIn. A rede social Academia.edu apresenta uma adesão muito fraca (M = 1,27), dado tratar-se de uma rede social relacionada com a investigação académica, esta fraca utilização pode ser explicada pelo facto dos respondentes apenas 4,28% estarem a frequentar um curso de Doutoramento.

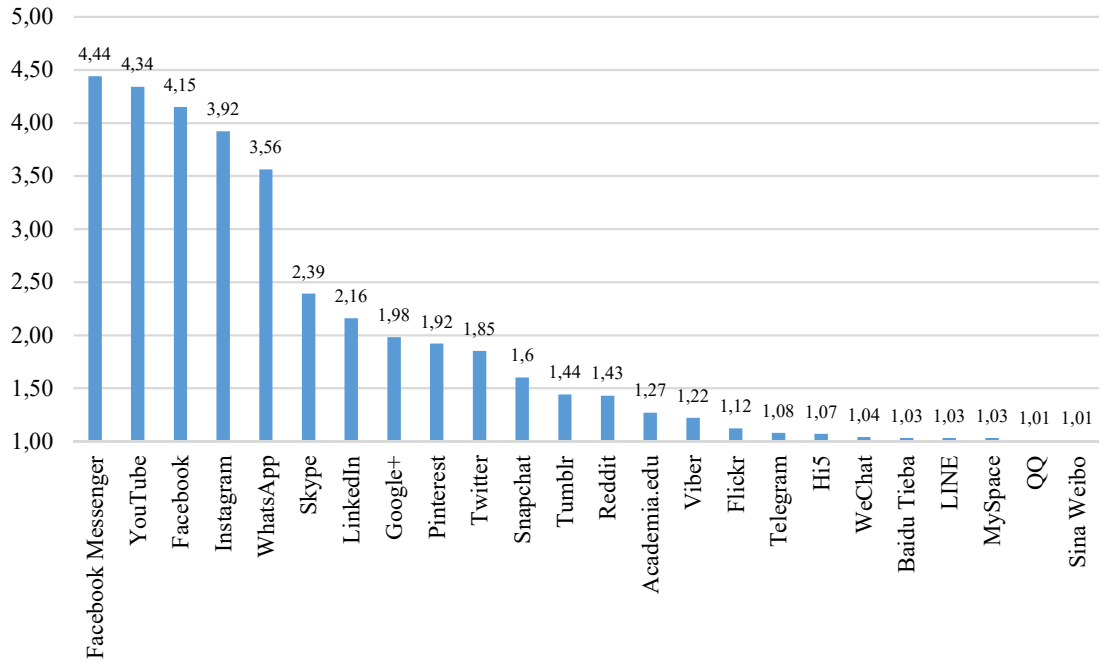

Figura 13 - Utilização das redes sociais

Da análise detalhada das redes sociais mais utilizadas, verifica-se a existência de discrepâncias na utilização destas redes em função do escalão etário do aluno.

Na Figura 14 verifica-se com especial incidência que o Instagram e o YouTube são bastante mais utilizados por alunos com idades até aos 20, sendo que esta utilização vai decrescendo à medida que o escalão etário sobe. Apesar de se verificar, regra geral, uma menor utilização das redes sociais nos escalões etários acima dos 30 anos, no caso do Instagram e do YouTube o diferencial de utilização entre os indivíduos com mais de 30 anos e os indivíduos com idades até 20 anos é francamente maior.

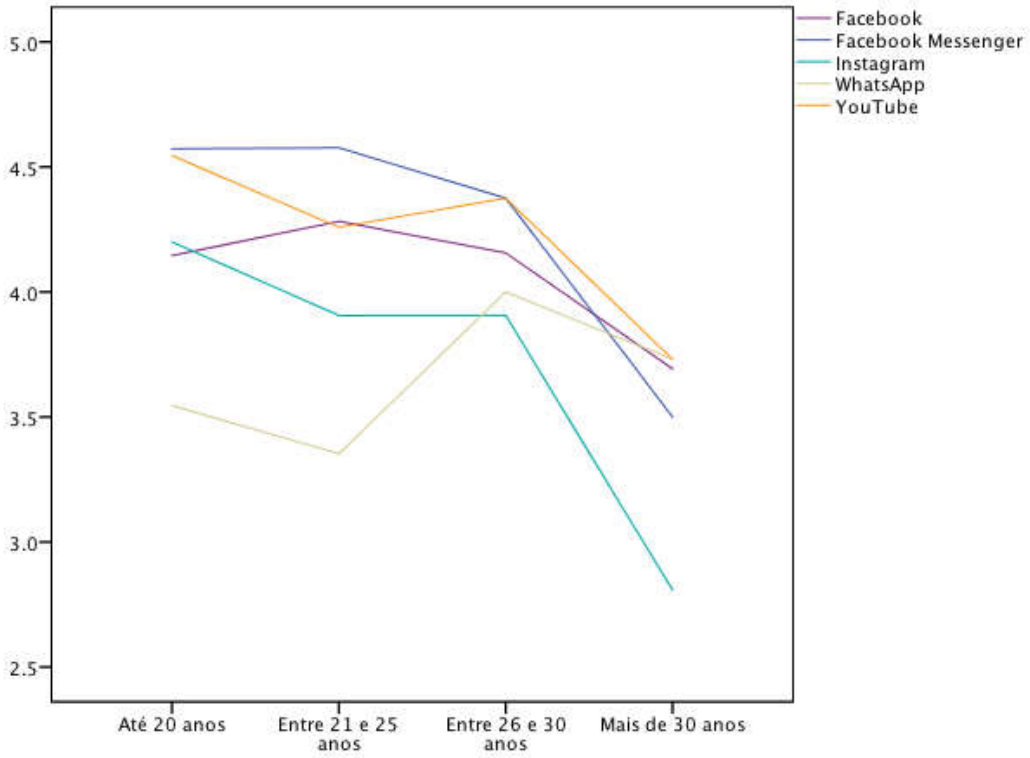

Figura 14 – Utilização das redes sociais em função de escalão etário

Os dois casos do Instagram e do YouTube são consubstanciados por correlações negativas fracas (ró [ρ] de Spearman) entre a idade e a frequência de utilização (Tabela 4), o que indica que à medida que a idade diminui, a frequência de utilização de ambos aumenta.

Tabela 4 - Correlação de Idade com redes sociais mais utilizadas

		Idade
Facebook	Coeficiente de Correlação	-.003
	Sig. (bicaudal)	.962
	N	253
Facebook Messenger	Coeficiente de Correlação	-.130*
	Sig. (bicaudal)	.039
	N	253
Instagram	Coeficiente de Correlação	**-.223*****
	Sig. (bicaudal)	,000
	N	253
WhatsApp	Coeficiente de Correlação	.067
	Sig. (bicaudal)	.287
	N	253
YouTube	Coeficiente de Correlação	**-.257*****
	Sig. (bicaudal)	,000
	N	253

*** p < 0,001; ** p < 0,01; * p < 0,05

Por fim verifica-se que apenas a rede social WhatsApp não sofre uma redução da sua utilização à medida que a idade dos alunos aumenta. Nas restantes redes mais utilizadas todas elas sofrem uma acentuada redução na frequência de utilização nos alunos com mais de 30 anos.

Em seguida temos o quarto objetivo da dissertação, *determinar os comportamentos típicos dos estudantes nas redes sociais*, basicamente para que usam e porque usam os estudantes as redes sociais. Para esta análise foram utilizados os dados recolhidos na pergunta 4 da parte II do questionário (cf. Apêndice D). Foi perguntado com que frequência os alunos executam diversos tipos de atividades nas redes sociais, com uma escala de 1 (nunca) a 5 (muito frequentemente). A atividade mais frequente nas redes sociais é, a conversa através de mensagens instantâneas (M = 4,39), em segundo lugar vem a atividade de ouvir música e vídeos (M = 3,80), seguido pela partilha de gostos/*likes* (M = 3,78). As atividades com a menor frequência são dar donativos (M = 1,55), fazer diários de viagens (M = 1,71), partilhar a localização (M = 1,74), partilhar pensamentos e sentimentos (M = 1,76) e sugerir amigos (M = 1,78). Em mais de metade das atividades sugeridas os alunos responderam que em média "quase nunca" (M < 3) as fazem nas redes sociais. Esta resposta pode indiciar que os alunos como utilizadores das redes sociais maioritariamente só consomem informação, contudo as restantes pessoas que usam as redes sociais, partilham informação. Confirma-se o que já se presenciou no *focus group*, uma dissociação entre o aluno como utilizador de rede social e o aluno como pessoa, apresentando comportamentos distintos relativamente à partilha de informação em cada um dos papeis (Barnes, 2006; Kokolakis, 2017).

Para a identificação dos comportamentos típicos nas redes sociais, foi realizada uma ACP com os itens da questão 4. Esta ACP permite-nos identificar as principais dimensões para a determinação dos comportamentos típicos dos estudantes nas redes sociais (Tabela 5), neste caso, seis fatores, que correspondem às dimensões representativas dos comportamentos típicos nas redes sociais.

O primeiro fator (29,80% de variância total explicada, com alfa de Cronbach α = 0,821) agrupa os itens referentes à partilha de conteúdos de terceiros na rede social.

O segundo fator (8,35% de variância total explicada, com alfa de Cronbach $\alpha = 0,778$) agrupa os itens referentes à participação na rede através de partilha de conteúdos próprios (*posts*, *likes*, pedidos de amizade, etc).

O terceiro fator (7,04% de variância total explicada, com alfa de Cronbach $\alpha = 0,713$) agrupa os itens referentes aos grupos, à integração em grupos e comunidades.

O quarto fator (5,31% de variância total explicada, com alfa de Cronbach $\alpha = 0,692$) agrupa os itens referentes a manter contacto e conversar com amigos e familiares.

O quinto fator (4,80% de variância total explicada, com alfa de Cronbach $\alpha = 0,715$) agrupa os itens referentes às notícias, atualidades e contacto com marcas e empresas.

O sexto fator (4,53% de variância total explicada, com alfa de Cronbach $\alpha = 0,622$) agrupa os itens referentes aos jogos online, concursos e aplicações usadas dentro das redes sociais.

Tabela 5 - Estrutura fatorial das dimensões associadas aos comportamentos típicos nas redes sociais

	Componentes					
	Partilha	**Participar**	**Grupos**	**Conversar**	**Noticias**	**Jogos**
Partilhar links, notícias e blogs	,796	,109	,122	,174	,247	,006
Partilhar música e filmes	,781	,032	,084	,309	-,037	,211
Partilhar conteúdos cómicos	,746	,204	,098	,057	,120	,175
Partilhar pensamentos e sentimentos	,669	,152	,133	,121	,002	,133
Sugerir amigos	,578	,163	,177	-,186	,121	,066
Aceitar e fazer pedidos de amizade	,048	,705	,262	,044	,122	,085
Comentar "posts" e mensagens de outras pessoas	,340	,669	,149	,205	,010	,221
Fazer Gostos/*Likes*/*Love*, etc,	,277	,635	-,049	,262	,258	,128
Identificar amigos	,194	,626	,322	,162	,160	,121
Criar e dinamizar grupos de interesse ou comunidades	,152	-,012	,786	,203	-,100	,138
Fazer parte de grupos de interesse ou comunidades	,120	,151	,642	,042	,308	-,150
Fazer inquéritos e sondagens	,173	,261	,629	-,056	,097	,041
Criar e agendar eventos	,137	,211	,603	,220	-,097	,341

	Componentes					
	Partilha	**Participar**	**Grupos**	**Conversar**	**Noticias**	**Jogos**
Manter contacto com amigos e familiares distantes	,080	,267	,180	,667	,243	-,135
Ouvir música e vídeos	,166	-,052	,060	,635	,138	,310
Manter contacto com antigos amigos	,105	,281	,129	,624	,287	-,203
Conversas através de mensagens instantâneas (Chat)	,050	,423	,069	,513	,049	,134
Ver notícias e atualidades	,131	,065	,074	,195	,776	,064
Seguir informação sobre produtos, serviços e empresas	,079	,160	,088	,164	,733	,127
Seguir personalidades públicas ou ídolos	,157	,307	-,115	,286	,559	,330
Jogar jogos on-line	,132	,107	,194	-,052	,027	,656
Partilhar a minha localização	,219	,331	-,090	,038	,111	,578
Participar em concursos, sorteios e inquéritos	,076	,102	-,021	,426	,207	,550
Usar aplicações oferecidas dentro da rede social	,358	,025	,287	-,068	,340	,506
Valores próprios	7,15	2,00	1,69	1,27	1,15	1,08
Variância Explicada (%)	29,80	8,35	7,04	5,31	4,80	4,53
Percentagem Acumulada	29,80	38,15	45,20	50,51	55,32	59,85
Alfa de Cronbach (α)	0,821	0,778	0,713	0,692	0,715	0,622

Nota: Resultado da ACP: matriz após rotação varimax, com normalização Kaiser, convergente em 9 iterações.
Medida KMO = 0,861, Teste de Bartlett = 1871,691, Significância = 0,000

O quinto objetivo desta dissertação pretende *verificar a importância das redes sociais na vida pessoal, académica e profissional dos estudantes*, para responder a este objetivo foram usadas as respostas à pergunta 5 da Parte II do questionário (cf. Apêndice D). A questão 5 expõe um conjunto de 20 afirmações relacionadas com as finalidades, usos e importância das redes sociais às quais foi pedido aos alunos que classificassem em função da sua importância, foi usada uma escala de 1 (nada importante) a 5 (muito importante).

O valor médio registado a todas as questões situou-se entre os escalões pouco importante e moderadamente importante (M = 2,60), este valor à primeira vista pode indiciar que em média para os alunos da amostra as redes sociais são, quanto muito,

moderadamente importantes, contudo os valores previamente registados na frequência de utilização das redes sociais de alguma forma podem contrariar esta ideia.

A razão mais importante para o uso, finalidade ou importância das redes sociais nos dados recolhidos prende-se com a possibilidade de estas agilizarem o contacto com colegas e professores (M = 3,80), em segundo lugar aparece a capacidade das redes sociais em reunir rapidamente e praticamente em tempo real, informação e noticias atualizadas sobre o mundo que rodeia os alunos (M = 3,64), uma outra razão vista como moderadamente importante foi a possibilidade de construir e manter uma rede de contactos profissionais (M = 3,38), a baixa importância deste item pode de certa forma indiciar o facto de a maioria dos alunos estarem inscritos no 1º ano dos seus cursos, ainda com uma baixa sensibilidade para o mercado de trabalho, como já antes discutimos. Em quarto lugar de importância surge a possibilidade de organizar grupos de trabalho para atividades de estudo (M = 3,36).

Por outro lado, no extremo oposto dos itens de menor importância temos o, orgulho em divulgar que estou nas redes sociais e a possibilidade de ter um perfil muito detalhado nas redes sociais (ambos com M = 1,63), divulgar dados pessoais online para satisfazer as necessidades sociais obteve em média também uma importância baixa (M = 1,66), usar as redes sociais para partilhar o dia-a-dia (M = 1,69) e divulgar dados pessoais online para cultivar bons relacionamentos (M = 1,74). Em suma todos estes itens sugerem que de alguma forma poderá até existir um pudor em assumir o uso das redes sociais, contudo as frequências de utilização indicam que os inquiridos as usam bastante!

Como forma de identificar a importância dada às redes, foi efetuada uma ACP com os itens da questão 5. Nesta ACP foi possível identificar dimensões para a importância das redes sociais na vida dos estudantes (Tabela 6). Foram identificados três fatores, que correspondem às dimensões associadas à importância dada às redes sociais.

O primeiro fator (39,20% de variância total explicada, com alfa de Cronbach α = 0,888) agrupa os itens referentes a cultivar relacionamentos e partilhar informação pessoal.

O segundo fator (13,58% de variância total explicada, com alfa de Cronbach α = 0,854) agrupa os itens referentes ao lazer, rotina diária e recolha de informação.

O terceiro fator (9,00% de variância total explicada, com alfa de Cronbach α = 0,745) agrupa os itens referentes à rede profissional, *networking* e grupos de trabalho.

Tabela 6 - Estrutura fatorial das dimensões associadas à importância dada às redes sociais

	Componentes		
	Relacionamentos	**Lazer**	**Profissional**
Divulgar dados pessoais online satisfaz as minhas necessidades sociais (de alguma forma)	,862	,052	,102
Divulgar dados pessoais online ajuda-me a cultivar bons relacionamentos	,789	,035	,243
Ter um perfil muito detalhado nas redes sociais	,774	,162	,171
Partilhar coisas sobre mim com contactos casuais	,752	,186	,150
Partilhar o meu dia-a-dia	,723	,240	,150
Tenho orgulho em dizer às pessoas que estou nas redes sociais	,681	,281	,030
Relaxar e descomprimir nas redes sociais	,247	,817	,005
Diversão ao passar tempo nas redes sociais	,276	,739	,130
As redes sociais online fazem parte da minha rotina diária	,260	,700	,280
Reunir rapidamente e em tempo real informação ou notícias atualizada/s sobre a minha cidade, país ou mundo	-,097	,669	,219
Aproveitar ao máximo todos os momentos livres para verificar o estado nas redes sociais (na casa de banho, transportes públicos, filas de espera, etc...)	,359	,661	,097
Sinto que faço parte da comunidade da rede social que mais uso	,490	,589	,122
Agiliza o contacto com colegas e professores	-,125	,528	,441
Construir e manter uma rede de contactos profissionais	,015	,252	,841
Construir um perfil público com vista a maximizar a exposição e o *networking*	,327	,087	,740
Partilhar conteúdos relevantes para a minha atividade profissional	,285	,062	,715
Organizar grupos de trabalho para atividades de estudo	,167	,327	,460
Valores próprios	6,66	2,22	1,53
Variância Explicada (%)	39,20	13,05	9,00
Percentagem Acumulada	39,20	52,26	61,26
Alfa de Cronbach (α)	0,888	0,854	0,745

Nota: Resultado da ACP: matriz após rotação varimax, com normalização Kaiser, convergente em 6 iterações.
Medida KMO = 0,890, Teste de Bartlett = 1687,705, Significância = 0,000

O sexto e último objetivo é o estudo das *relações entre as dimensões encontradas sobre a segurança e privacidade, com os comportamentos típicos nas redes sociais*. É

este objetivo que pretende dar resposta ao projeto como um todo, neste objetivo pretende-se saber se existe uma relação entre conceitos latentes de privacidade e segurança e os tipos de utilização que os alunos fazem das redes sociais, em suma, se a preocupação com a privacidade e segurança condiciona (ou é condicionada) pela forma e os pelos tipos de utilização e importância atribuídos às redes sociais.

De forma a identificar estas correlações foram feitos dois estudos de correlações bivariadas, um entre as dimensões da privacidade e as dimensões da segurança e comportamentos típicos nas redes sociais (Tabela 7) e outro entre as dimensões da segurança e os comportamentos típicos nas redes sociais (Tabela 8), em ambos os estudos foram observadas várias correlações significativas.

Na exploração de correlações com a esfera da privacidade (Tabela 7), como se antevia, verificou-se que em todas as dimensões relativas à segurança da informação (Conhecimento, Segurança e Proteção) existem relações moderadas crescentes (entre ,443 e ,541) com as dimensões relativas à privacidade (Privacidade e Controlo), isto é, à medida que os alunos atribuem maior importância à sua segurança dos dados também aumenta a importância dada às perceções relativas à privacidade.

Tabela 7 - Correlação de dimensões da privacidade com dimensões de segurança e comportamentos típicos nas redes sociais

		Privacidade da rede social	Capacidade de controlo da informação privada
Privacidade da rede social	Coeficiente de Correlação	1	
	N	232	
Capacidade de controlo da informação privada	Coeficiente de Correlação	**,477*****	1
	Sig. (bicaudal)	,000	
	N	232	232
Conhecimento de quem pode aceder à informação privada	Coeficiente de Correlação	**,517*****	**,482*****
	Sig. (bicaudal)	,000	,000
	N	219	219
Segurança da informação arquivada na rede social	Coeficiente de Correlação	**,455*****	,**541*****
	Sig. (bicaudal)	,000	,000
	N	219	219
Mecanismos de proteção reforçados na rede social	Coeficiente de Correlação	**,435*****	**,443*****
	Sig. (bicaudal)	,000	,000
	N	219	219

		Privacidade da rede social	Capacidade de controlo da informação privada
Partilha de conteúdos de terceiros	Coeficiente de Correlação	-,139*	**-,206****
	Sig. (bicaudal)	,043	,002
	N	213	213
Participar nas redes sociais	Coeficiente de Correlação	,015	-,083
	Sig. (bicaudal)	,833	,227
	N	213	213
Integração em grupos e comunidades	Coeficiente de Correlação	-,088	-,121
	Sig. (bicaudal)	,199	,077
	N	213	213
Conversar e manter contacto com amigos	Coeficiente de Correlação	,033	,017
	Sig. (bicaudal)	,637	,807
	N	213	213
Noticias, Atualidades e contacto com marcas e empresas	Coeficiente de Correlação	,021	-,048
	Sig. (bicaudal)	,763	,487
	N	213	213
Jogos online, concursos e aplicações usadas nas redes sociais	Coeficiente de Correlação	-,090	-,129
	Sig. (bicaudal)	,192	,059
	N	213	213
Cultivar relacionamentos e partilhar informação	Coeficiente de Correlação	**-,277*****	**-,277*****
	Sig. (bicaudal)	,000	,000
	N	200	200
Lazer, rotina e recolha de informação	Coeficiente de Correlação	,060	-,009
	Sig. (bicaudal)	,403	,897
	N	200	200
Rede profissional, *networking* e grupos de trabalho	Coeficiente de Correlação	,035	-,077
	Sig. (bicaudal)	,619	,277
	N	200	200

*** p < 0,001; ** p < 0,01; * p < 0,05

Quanto aos comportamentos nas redes sociais, assiste-se ao aparecimento de correlações fracas inversas (-,277) entre a importância dada à privacidade e o uso das redes sociais para cultivar relacionamentos e partilhar informação, por outras palavras, quanto maior for a apetência para a criação de relacionamentos e partilha de informação nas redes sociais menor é a importância dada à privacidade. Ainda neste domínio verificou-se a ocorrência de uma relação fraca inversa (-.206) entre a capacidade de

controlo da informação e a partilha de conteúdo de terceiros, quer isto dizer, que os alunos que usam as redes sociais principalmente para partilhar conteúdos de outros, de forma ligeira, tendem a atribuir menor importância à capacidade de controlar a sua informação privada. Esta correlação pode ser explicada pelo fato de os alunos que maioritariamente não partilham conteúdos privados não vêm tanta necessidade em poder controlar essa mesma informação.

No âmbito do estudo das correlações entre as dimensões da segurança (Conhecimento, Segurança e Proteção) e os comportamentos típicos nas redes sociais (Tabela 8) à semelhança do que se verificou com as dimensões da privacidade, verifica-se a existência de uma relação fraca inversa (-,217) entre a importância atribuída à segurança da informação arquivada na rede social e o uso das redes sociais para cultivar relacionamentos e partilhar informação, isto é, quanto maior for a apetência para a criação de relacionamentos e partilha de informação nas redes sociais menor é a importância dada à segurança da informação arquivada na rede social. Esta correlação pode ser explicada pelo facto de os indivíduos cujo principal *driver* para a utilização das redes sociais seja a criação de relações sociais e a partilha de informação, na realidade não estão assim tão preocupados com a segurança da informação, isto porque, afinal, o principal objetivo é a partilha da informação e não a segregação da mesma.

Tabela 8 - Correlação de dimensões de segurança com os comportamentos típicos nas redes sociais

		Conhecimento de quem pode aceder à informação privada	Segurança da informação arquivada na rede social	Mecanismos de proteção reforçados na rede social
Conhecimento de quem pode aceder à informação privada	Coeficiente de Correlação	1		
	N	219		
Segurança da informação arquivada na rede social	Coeficiente de Correlação	**,631*****	1	
	Sig. (bicaudal)	,000		
	N	219	219	
Mecanismos de proteção reforçados na rede social	Coeficiente de Correlação	**,583*****	**,573*****	1
	Sig, (bicaudal)	,000	,000	
	N	219	219	219
	Coeficiente de Correlação	-,070	-,010	,011
	Sig, (bicaudal)	,307	,888	,868

Partilha de conteúdos de terceiros	N	213	213	213
Participar nas redes sociais	Coeficiente de Correlação	,012	,040	,046
	Sig, (bicaudal)	,863	,561	,500
	N	213	213	213
Integração em grupos e comunidades	Coeficiente de Correlação	-,061	-,084	-,072
	Sig, (bicaudal)	,374	,224	,299
	N	213	213	213
Conversar e manter contacto com amigos	Coeficiente de Correlação	,048	,096	,047
	Sig, (bicaudal)	,485	,163	,498
	N	213	213	213
Noticias, Atualidades e contacto com marcas e empresas	Coeficiente de Correlação	,045	,016	-,015
	Sig, (bicaudal)	,515	,813	,828
	N	213	213	213
Jogos online, concursos e aplicações usadas nas redes sociais	Coeficiente de Correlação	-,104	-,088	-,025
	Sig, (bicaudal)	,130	,200	,714
	N	213	213	213
Cultivar relacionamentos e partilhar informação	Coeficiente de Correlação	-,162*	**-,217****	-,085
	Sig, (bicaudal)	,022	,002	,232
	N	200	200	200
Lazer, rotina e recolha de informação	Coeficiente de Correlação	,113	,148*	,101
	Sig, (bicaudal)	,111	,036	,156
	N	200	200	200
Rede profissional, *networking* e grupos de trabalho	Coeficiente de Correlação	-,010	-,024	,013
	Sig, (bicaudal)	,894	,735	,850
	N	200	200	200

*** p < 0,001; ** p < 0,01; * p < 0,05

Por fim uma outra questão relevante, a ausência de correlações estatisticamente significativas entre as dimensões da privacidade e segurança e o uso das redes sociais para efeitos de *networking* e para a criação de redes profissionais, vemos que no domínio do uso profissional e académico das redes sociais os alunos não atribuem importância à privacidade e segurança dos dados. Uma possível explicação, é o facto de a amostra deste estudo ser composta por cerca de 40% de alunos inscritos no 1º ano dos seus cursos e por mais de 45% dos alunos estarem a frequentar uma Licenciatura, este distanciamento do mundo profissional de uma percentagem muito relevante dos inquiridos de certo que

poderá estar na origem desta aparente despreocupação da privacidade e segurança com o uso das redes sociais no âmbito profissional.

Capítulo 6 – Análise e discussão dos resultados

6.1. Discussão por fases

Na fase exploratória deste trabalho foram desenvolvidos dois estudos complementares, um *focus group* e entrevistas com especialistas na área das redes sociais. O objetivo tanto do *focus group* como das entrevistas foi o de estudar a adequação dos temas resultantes da revisão da literatura às perceções tanto de um grupo de alunos como de especialistas no terreno, estes temas mais tarde serviram de base para a elaboração de um questionário, usado na fase inferencial e correlacional da presente investigação.

Dos resultados obtidos no *focus group*, foi possível identificar diversos conceitos e as suas inter-relações, estas por sua vez confirmaram algumas das perceções de privacidade e segurança dos estudantes no âmbito das redes sociais. Em primeiro lugar verificou-se que existe a noção que o que liga as empresas aos utilizadores são as redes sociais, existe a noção que os utilizadores sabem o que são redes sociais, e que as usam para partilhar informação por vezes privada. Já as empresas usam as redes sociais para fins comerciais. A partilha de informação dos utilizadores está muito centrada no momento, isto é, a partilha de informação é feita em função de acontecimentos estáticos no tempo, tempo esse que é encarado pelos utilizadores como já não pertencendo ao presente e por conseguinte estando já fora de alcance. Existe, contudo, uma preocupação crescente que esse passado possa ressurgir e poder ter impactos negativos.

Apesar dos riscos inerentes à perda de privacidade nas redes sociais, os alunos simplesmente "desistem de querer saber" verifica-se uma apatia semiconsciente relativamente à privacidade e segurança. Por fim o *focus group* evidenciou uma dicotomia muito presente na revisão de literatura, utilizador *versus* pessoa, como que a atitude relativa à privacidade e o comportamento relativo à privacidade são vistos de formas completamente diferentes.

As entrevistas tiveram como objetivo a obtenção de outra visão sobre os mesmos temas abordados no *focus group*, como que moderadores da informação compilada no *focus group*. Nas entrevistas foi reforçada a visão do *focus group* que as redes sociais e as pessoas se interligam, isto é, que as pessoas são as redes sociais, diminuindo assim a fronteira entre a vida digital e a vida social das pessoas. As entrevistas também permitiram reunir a ideia que os utilizadores das redes sociais não seguem padrões de uso com vista a manter e reforçar a sua privacidade e segurança nas redes sociais, antes pelo contrário.

Enquanto que no *focus group* o impacto das redes sociais no futuro profissional dos alunos já se nota de alguma forma, nas entrevistas com professores universitários o foco dos impactos negativos das redes sociais na atividade laboral é muito maior. Também nas entrevistas aparece o conceito de pessoas separado, neste caso, do conceito de alunos, as entrevistas passam a ideia de mudança nas mentalidades relativas à privacidade e segurança nas redes sociais online, sugerindo que na sua maioria os alunos universitários já assumem comportamentos com menos riscos de exposição que a população em geral.

Nos resultados obtidos na fase inferencial e correlacional foi possível identificar que do ponto de vista das perceções de privacidade existem duas grandes dimensões: (i) a privacidade providenciada pela rede social e (ii) a capacidade de controlar a informação privada, em ambos os índices foram registados níveis de importância muito altos (ver Tabela 9) , sendo a grande maioria dos inquiridos (>85%) de opinião que ambos os índices são importantes ou muito importantes (cf. Apêndice F).

Tabela 9 - Média e desvio padrão dimensões perceção de privacidade

	N	Média	Desvio Padrão
Privacidade da rede social	232	4,63	,48
Capacidade de controlo da informação privada	232	4,61	,50

Nas dimensões das perceções dos alunos da segurança foram validados três componentes: (i) o conhecimento de quem pode aceder à informação, (ii) a segurança da informação arquivada na rede social e (iii) os mecanismos de proteção reforçada das redes sociais, em todos estes índices verificaram-se valores de importância também muito altos (ver Tabela 10), a maioria dos inquiridos (>80%) tem opinião que todos os índices relativos à segurança são importantes ou muito importantes (cf. Apêndice F).

Tabela 10 - Média e desvio padrão dimensões perceção de segurança

	N	Média	Desvio Padrão
Conhecimento de quem pode aceder à informação privada	219	4,59	,47
Segurança da informação arquivada na rede social	219	4,64	,41
Mecanismos de proteção reforçados na rede social	219	4,52	,49

Relativamente às redes sociais online mais usadas, vemos que na amostra a rede social mais utilizada é o Facebook Messenger, seguido pelo YouTube, Facebook, Instagram e WhatsApp (ver Figura 13). Desde que se deu a desagregação do Facebook Messenger da plataforma Facebook, passando a ser possível, através da aplicação móvel dedicada usar o Facebook Messenger sem ter que estar no Facebook, que ambas as plataformas começaram a apresentar ritmos de adesão e crescimento distintos, essa suspeita é confirmada aqui nos valores registados neste estudo. Outro indício que este estudo de certa forma confirma, é que o Facebook como rede social não está a ter tanta adesão nas camadas mais jovens (abaixo dos 20 anos) como tem nas camadas acima. Contrariamente o YouTube e o Instagram são mais usados pelas camadas mais jovens (até aos 20 anos) e subsequentemente menos usados pelos restantes escalões etários. Assiste-se a um incremento na utilização do YouTube e do Instagram em detrimento do Facebook. Assiste-se ao crescimento das redes sociais que privilegiam mais o contacto direto por meio de *chat* e a partilha do "momento" em vez das redes que dão mais enfoque à construção de uma *persona* online.

Como principais dimensões para os comportamentos típicos dos estudantes nas redes sociais foram identificados seis padrões distintos: (i) partilha de conteúdos de terceiros, (ii) participação através da partilha de conteúdos próprios (iii) pertença a grupos e comunidades, (iv) manter contacto com amigos e familiares, (v) ver noticias, atualidades, marcas e empresas e (vi) jogar, participar em concursos e usar *apps* sociais. Contrariamente ao que seria de esperar, os valores de frequência de utilização das redes sociais para cada um dos tipos de utilização são baixos (ver Tabela 11), com a quase maioria das respostas (>40%) a situar-se entre o quase nunca e o às vezes (cf. Apêndice F). Peculiarmente os tipos de utilização mais frequentes (participar nas redes sociais, conversar e manter contacto com amigos) são também os que mais expõem a privacidade dos utilizadores nas redes sociais.

Tabela 11 - Média e desvio padrão dimensões tipos de utilização das redes sociais

	N	Média	Desvio Padrão
Partilha de conteúdos de terceiros	213	2,16	,82
Participar nas redes sociais	213	3,24	,77
Integração em grupos e comunidades	213	2,63	,79

Conversar e manter contacto com amigos	213	3,83	,76
Noticias, Atualidades e contacto com marcas e empresas	213	3,12	,88
Jogos online, concursos e aplicações usadas nas redes sociais	213	1,94	,68

Do ponto de vista da importância atribuída às redes sociais na vida pessoal, académica e profissional dos estudantes foram identificados três grandes componentes: (i) cultivar relacionamentos e partilhar informação, (ii) lazer, rotina diária e recolha de informação e (iii) a criação de uma rede profissional, *networking* e grupos de trabalho. Os resultados obtidos (Tabela 12) evidenciam que em primeiro lugar de importância as redes sociais são locais para lazer e para recolha de informação, em segundo lugar as redes sociais são importantes para fazer parte de grupos de trabalho e para dinamizar as redes profissionais, em último lugar bastante distanciado está o uso das redes sociais para partilhar informação tendo esta última dimensão uma categorização de nada importante quase a pouco importante.

Tabela 12 - Média e desvio padrão dimensões importância das redes sociais na vida pessoal, académica e profissional

	N	**Média**	**Desvio Padrão**
Cultivar relacionamentos e partilhar informação	200	1,69	,72
Lazer, rotina e recolha de informação	200	3,13	,79
Rede profissional, *networking* e grupos de trabalho	200	3,09	,85

Constata-se mais uma vez que os alunos não usam as redes sociais para partilhar informação, à primeira vista esta é uma atitude que combina com os valores de importância atribuídos à privacidade e segurança, contudo nos tipos de uso mais frequentes vemos exatamente o oposto onde os tipos de uso de partilha de informação são os mais frequentes, estes dados vêm integralmente comprovar o que foi observado no *focus group*, a atitude dos alunos perante a privacidade é diferente do comportamento perante a mesma, confirma-se na nossa amostra e no *focus group* a ocorrência do paradoxo da privacidade.

6.2. Discussão global de resultados

Neste trabalho ficou patente a importância que os estudantes universitários atribuem à privacidade e segurança dos seus dados pessoais quando utilizam as redes sociais online. Contudo, os seus comportamentos nas redes sociais não estão em harmonia com a importância que atribuem à privacidade (Barnes, 2006; Boyd, 2014; Boyd & Hargittai, 2010; Kokolakis, 2017).

Os estudantes sabem que as redes sociais são as próprias pessoas, sabem também que as empresas e organizações que gravitam nas redes sociais não fazem parte delas, mas que são fonte de informação. A informação que é partilhada nas redes sociais pelos estudantes foca-se primordialmente num determinado momento não pretendendo representar o *continuum* da vida do estudante. Esta partilha efémera de informação, aparentemente desconexa leva a que o aluno desista, de uma forma porventura consciente, da imposição de comportamentos que conduzem à privacidade em prejuízo da exposição social (Hargittai & Marwick, 2016).

Estes conceitos qualitativos foram validados num estudo inferencial e correlacional onde foram identificadas do ponto de vista da privacidade, da segurança, do tipo de utilização das redes sociais e da importância atribuída às redes sociais diversas dimensões que quando analisadas como um todo, não estão em sintonia. Por um lado, os alunos mostram-se muito preocupados com a sua privacidade, a sua segurança, afirmando que não usam as redes sociais para partilhar informação própria nem para cultivar relacionamentos. Por outro, afirmam usar com mais frequência as redes sociais para partilhar informação pessoal, para conversar e manter contactos. Os alunos também indicam usar com elevada frequência (frequentemente e muito frequentemente) as redes sociais, nomeadamente (por ordem decrescente) o Facebook Messenger, o YouTube, o Facebook, o Instagram e o WhatsApp.

Entre a população deste estudo assiste-se a uma diminuição da apetência do uso do Facebook nas camadas mais jovens (abaixo dos 20 anos) substituindo o seu uso pelas redes Instagram e YouTube. No caso do YouTube o seu crescimento nos indivíduos socialmente mais ativos é acentuado levando em alguns casos até mesmo a preterir o consumo de Televisão em prol do YouTube (Haridakis & Hanson, 2009).

Do ponto de vista da privacidade os alunos dividem o conceito em dois pilares, a privacidade da própria rede social e a capacidade de controlar o fluxo da informação na

rede social (Park, 2015). Na segurança são reconhecidos três princípios fundamentais pelos alunos, o conhecimento de quem pode aceder à informação, a segurança do arquivo da informação e existência de mecanismos de proteção da informação. Os comportamentos dos alunos nas redes sociais dividem-se em partilhar conteúdos de terceiros, participar partilhando informação própria, fazer parte de grupos, conversar de forma direta e interativa, recolher informação de atualidade, sobre empresas, produtos e serviços e por último jogar e usar *apps* sociais.

Relativamente à importância das redes sociais na vida dos estudantes, esta importância divide-se em três conceitos: criação de relacionamentos, lazer e utilização profissional e para grupos de trabalho.

Por fim, foi possível identificar correlações significativas entre a privacidade e a segurança, isto é, as perceções de privacidade dos alunos estão associadas de forma moderada a forte às perceções de segurança, reconhecendo assim os alunos que os conceitos de privacidade e segurança são indissociáveis. Por outro lado, verificaram-se correlações entre a importância da privacidade e a segurança da informação com o uso das redes sociais para cultivar relacionamentos e partilhar informação. Pelo que, em consciência, os alunos sabem que usar as redes sociais para partilhar informação conduz à redução da privacidade e à diminuição da segurança dos seus dados. Porém relembramos que a maioria dos alunos não considera importante o uso das redes sociais para cultivar relacionamentos e partilhar informação. Ao mesmo tempo, dizem que usam as redes sociais para conversar e participar nas redes sociais com conteúdos pessoais, mas esta partilha já não apresenta qualquer correlação com a perda de privacidade ou de segurança. Verifica-se desta forma a dicotomia entre a atitude dos alunos perante a privacidade e segurança e os seus comportamentos nas redes sociais.

Capítulo 7 – Conclusões

7.1. Principais conclusões

No rescaldo dos recentes eventos relativos ao assalto a milhões de contas de utilizadores, e à fuga de dados que ocorreram no Facebook, dos quais o mais mediático foi o escândalo associado à Cambridge Analytica (Greenfield, 2018), que expôs as sérias implicações que podem ocorrer sobre a recolha de informação privada/pessoal das redes sociais, a importância deste tipo de trabalhos é crescente, para difundir e sensibilizar a comunidade em geral, e os reguladores em particular, para os potenciais perigos da invasão das redes sociais na esfera da vida privada de cada cidadão.

Da análise aos conceitos recolhidos sobre privacidade, segurança e redes sociais que emergem deste trabalho, chega-se a diversas conclusões. Em primeiro lugar, o que liga as empresas e os utilizadores, hoje em dia, são as redes sociais. As pessoas sabem o que são redes sociais e que tipos de redes sociais existem, assiste-se até a uma possibilidade de mudança para dar origem a que novos comportamentos relativos à privacidade possam começar a acontecer nas camadas mais jovens. Atualmente ainda se verifica um alheamento porventura consciente de ignorar a preocupação da perda de privacidade nas redes sociais (Hargittai & Marwick, 2016).

Entretanto, os estudantes partilham e reúnem informação dos seus momentos e dos momentos da sua rede social. Estes momentos no tempo são encarados como pertença de um passado distante, quase como que desaparecem. Apesar de existir uma preocupação crescente para o futuro uso desta informação, que de certa forma poderá criar dificuldades e constrangimentos na próxima etapa da vida dos estudantes, a entrada no mercado de trabalho (Rosenblum, 2007).

Como constructos que representam a privacidade, na perceção dos estudantes, a privacidade assenta basicamente na capacidade do controlo do fluxo da informação. Confirma-se aqui a análise de que a privacidade é na realidade a capacidade de controlo sobre a informação, participando esta capacidade de controlo como um dos pilares para a adesão às redes sociais (Shin, 2010). Esta capacidade de controlo é assessorada pela segurança dos dados privados, e para os estudantes a segurança dos dados pode ser encarada como conseguir saber quem tem acesso a quê, como é que a informação é segura na rede e a existência de mecanismos de proteção reforçada, estes últimos no fim da lista de preferências dos estudantes.

Entre as redes sociais mais usadas, verificou-se que o Facebook já não está em primeiro lugar no ranking das preferências dos estudantes, assistindo-se a uma tendência de mudança do Facebook para o Instagram e YouTube, entre as camadas mais jovens de estudantes (Salomon, 2013); em estudos assiste-se a esta tendência desde 2016 (Smith & Anderson, 2018).

Os principais tipos de comportamentos identificados no uso das redes sociais dividem-se em dois grandes grupos; o uso da rede social para consumir conteúdo e a participação na rede social para partilhar conteúdo, conversar e fazer parte de comunidades. Concluímos que as atividades mais frequentes nas redes socias são a conversa com amigos e a partilha de informação. Apesar de indicarem uma frequência tímida, estamos seguramente na presença de utilizadores ativos em *networking* e comunicação nas redes sociais (Nentwich & König, 2014). Ora, os nossos utilizadores de redes sociais que se assumem como "ativos em *networking* e comunicação", indicam que do ponto de vista de importância o menos importante é partilhar informação. As mesmas pessoas que se assumem como utilizadores ativos das redes sociais afirmam também que nestas o mais importante não é a possibilidade de cultivar relacionamentos. Isto é, os estudantes assumem que usam as redes sociais, que não se orgulham desse facto e que partilham informação, contudo, não consideram isso como importante, o que, em suma, é um contrassenso.

É neste contrassenso que presenciamos o famoso paradoxo da privacidade (Barnes, 2006), que associado à noção do momento no presente, em evidência neste trabalho, nos transporta para a visão de que o referido paradoxo pode ser explicado pelo desfasamento das recompensas sociais no presente terem um peso maior nos comportamentos das pessoas nas redes sociais quando confrontadas com eventuais desvantagens (neste caso de falta de privacidade) no futuro distante (Hallam & Zanella, 2017).

Por fim, este trabalho mostra a discrepância que existe entre o papel do utilizador das redes sociais e o papel das pessoas como produtores e consumidores de informação, que são percecionados como sendo seres distintos, o que configura um caso típico de "nós e eles", atitude *versus* comportamento (Kokolakis, 2017), apesar de, evidentemente, todos os utilizadores serem, na verdade, pessoas.

Neste trabalho, não só foi possível verificar e justificar os (seis) objetivos propostos, como também foi possível responder à questão de investigação, na medida em que se verificou que os estudantes universitários atribuem (conceptualmente) grande

importância à privacidade e segurança da sua informação, contudo, na sua prática, quando usam as redes sociais, esta importância é relegada para segundo plano.

Conclui-se assim que existe uma efetiva distorção, ambivalência ou distância, entre as perceções que os estudantes universitários têm da sua exposição online, da salvaguarda da sua privacidade, e os reais comportamentos que exibem no uso diário das redes sociais. Em suma, verifica-se de vital importância a inclusão de materiais educativos na área das TIC, a começar mesmo no terceiro ciclo do ensino básico, que exponham, elucidem e suscitem a discussão entre os estudantes, sobre esta problemática.

7.2.Limitações e dificuldades

Sem dúvida que a maior dificuldade neste trabalho foi a recolha de informação em quantidade, qualidade e diversidade. O facto de os dados recolhidos apresentarem uma distribuição tão assimétrica relativamente ao género, inviabilizou a possibilidade de se usar o sexo como variável independente e assim levar a cabo estudos sobre a influência de género. A influência de género nas atitudes perante a privacidade nas redes sociais é um elemento onde inúmeros autores dispõem de visões distintas, com uns a defender que existem diferenças no comportamento perante a privacidade entre homens e mulheres (Acquisti & Gross, 2006; Bergström, 2015; Cecere et al., 2015; Hajli & Lin, 2016), e outros, o oposto (Boyd & Hargittai, 2010; Park, 2013).

Outra grande dificuldade foi o facto de durante a execução deste trabalho se ter assistido a uma mediatização da problemática entre a privacidade a segurança e as redes sociais. Quando esta dissertação foi projetada não estava na ordem do dia a problemática da fuga de dados do Facebook. Sem dúvida que esta mediatização terá tido o seu peso em algumas respostas de alguns participantes nas diversas etapas desta investigação.

7.3.Propostas para o futuro

Como propostas para futuros trabalhos na área em estudo, em primeiro lugar, sem dúvida que um estudo aprofundado e com uma elevada base de respondentes, para a validação da existência (ou não) de uma influência direta do uso das redes sociais nos processos de formação de opinião pública coletiva. Por exemplo, até que ponto poderá estar o modelo de participação eleitoral no processo democrático em risco de poder ser manipulado com sucesso pelos *social media*?

Em segundo lugar, poderá ser muito interessante o estudo da hipotética tendência da mudança no tipo de uso que é feito nas redes sociais, "*Moments vs Profile*". Cada vez mais se assiste a uma mudança nas preferências de uso, principalmente nas camadas mais jovens, em usar as redes sociais não como um repositório de gostos, afinidades, insígnias ou galhardetes, mas apenas como um local onde partilhar momentos, quase desprovidos de emoção ou sentimento, como que congelados no tempo[21].

[21] "All those moments will be lost in time, like tears in rain." In Deeley, M., & Scott, R. (1982). *Blade runner*. Estados Unidos: Warner Bros.

Bibliografia

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the facebook. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 4258 LNCS, pp. 36–58). https://doi.org/10.1007/11957454_3

Ahn, G.-J., Shehab, M., & Squicciarini, A. (2011). Security and Privacy in Social Networks. *IEEE Internet Computing*, *15*(3), 10–12. https://doi.org/10.1109/MIC.2011.66

Aldhafferi, N., Watson, C., & A.S.M, S. (2013). Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices. *International Journal of Security, Privacy and Trust Management*, *2*(2), 1–17. https://doi.org/10.5121/ijsptm.2013.2201

Andreassen, C. S., Torsheim, T., Brunborg, G. S., & Pallesen, S. (2012). Development of a Facebook Addiction Scale. *Psychological Reports*, *110*(2), 501–517. https://doi.org/10.2466/02.09.18.PR0.110.2.501-517

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9), 5. https://doi.org/10.5210/fm.v11i9.1394

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2015.07.025

Bilge, L., Strufe, T., Balzarotti, D., Kirda, E., & Antipolis, S. (2009). All Your Contacts Are Belong to Us : Automated Identity Theft Attacks on Social Networks. *Www 2009*, 551–560. https://doi.org/http://doi.acm.org/10.1145/1526709.1526784

Bonneau, J., & Preibusch, S. (2010). The privacy jungle: On the market for data protection in social networks. *Economics of Information Security and Privacy*, 1–45. https://doi.org/10.1007/978-1-4419-6967-5_8

Boyd, D. (2008). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *Convergence*, *14*(1), 13–20. https://doi.org/10.1177/1354856507084416

Boyd, D. (2014). *It's Complicated: The Social Lives of Networked Teens*. *It'S Complicated: the Social Lives of Networked Teens*. Yale University Press. https://doi.org/10.1007/s10615-014-0512-3

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

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, *15*(8). https://doi.org/10.5210/fm.v15i8.3086

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 154–165. https://doi.org/10.1002/asi.20459

Castells, M. (1996). *The Rise of the Network Society. The Information Age: Economy, Society, and Culture Volume I (Information Age Series)*. London: Blackwell.

Castells, M. (2002). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford University Press on Demand.

Cavoukian, A. (2011). Privacy by Design. *The 7 Foundational Principles*, 1–2. Retrieved from http://publication/uuid/9F8761B1-D114-42A3-9AF0-4521C5D78F2A

Cecere, G., Le Guel, F., & Soulié, N. (2015). Perceived Internet privacy concerns on social networks in Europe. *Technological Forecasting and Social Change*, *96*, 277–287. https://doi.org/10.1016/j.techfore.2015.01.021

Chen, H.-T., & Chen, W. (2015). Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 13–19. https://doi.org/10.1089/cyber.2014.0456

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*. https://doi.org/10.1002/ejsp.2049

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Americas Conference on Information Systems (AMCIS)*, *123*, 339–350. https://doi.org/10.1.1.148.9388

Ellison, N. B., & Boyd, D. (2013). Sociality through social network sites. *The Oxford Handbook of Internet Studies*, 151–172. https://doi.org/10.1093/oxfordhb/9780199589074.001.0001

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, *12*(4), 1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. https://doi.org/10.1016/j.chb.2008.08.006

Freitas, H., Oliveira, M., Jenkins, M., & Popjoy, O. (1998). The Focus Group, A Qualitative Research Method. *Isrc*, (010298), 1–22. https://doi.org/10.1016/j.watres.2013.02.032

Goodson, S. (2012). If You're Not Paying For It, You Become The Product.

Greenfield, P. (2018). The Cambridge Analytica files: the story so far. *The Guardian*.

Gressin, S. (2017). The Equifax data beach: What to do. *Federal Trade Commission*, (September), 8–10. Retrieved from https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Privacy in the Electronic Society 2005*, 11. https://doi.org/10.1145/1102199.1102214

Guha, S., Tang, K., & Francis, P. (2008). NOYB: Privacy in Online Social Networks. *Proceedings of the First Workshop on Online Social Networks*, 49–54. https://doi.org/http://doi.acm.org/10.1145/1397735.1397747

Hajli, N., & Lin, X. (2016). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics*, *133*(1), 111–123. https://doi.org/10.1007/s10551-014-2346-x

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2016.11.033

Hargittai, E. (2010). Digital Na(t)ives? Variation in internet skills and uses among members of the "net Generation." *Sociological Inquiry*, *80*(1), 92–113. https://doi.org/10.1111/j.1475-682X.2009.00317.x

Hargittai, E., & Marwick, A. (2016). "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication*, *10*(0), 21.

Haridakis, P., & Hanson, G. (2009). Social interaction and co-viewing with YouTube: Blending mass communication reception and social connection. *Journal of*

Broadcasting and Electronic Media. https://doi.org/10.1080/08838150902908270
Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic Commerce Research and Applications*, *9*(1), 50–60. https://doi.org/10.1016/j.elerap.2009.05.001
Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59–68. https://doi.org/10.1016/j.bushor.2009.09.003
Kaufman, L. (2009). Data security in the world of cloud computing, security and privacy. *Ieee*, *7*(4), 61–64.
Kitzinger, J. (1994). The methodology of Focus Groups: the importance of interaction between research participants. *Sociology of Health & Illness*, *16*(1), 103–121. https://doi.org/10.1111/1467-9566.ep11347023
Kitzinger, J. (1995). Introducing focus groups ' P. *BMJ : British Medical Journal*, *311*, 299–302.
Kizza, J. M. (2001). *Computer network security and cyber ethics*. McFarland.
Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*. https://doi.org/10.1016/j.cose.2015.07.002
Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110
Krasnova, H., Kolesnikova, E., Guenther, O., & Günther, O. (2009). "It Won't Happen To Me!": Self-Disclosure in Online Social Networks. *Amcis 2009 Proceedings*, 343. https://doi.org/10.7892/boris.47460
Krishnamurthy, B., & Wills, C. E. (2008). Characterizing privacy in online social networks. *Proceedings of the First Workshop on Online Social Networks (WOSP '08)*, 37–42. https://doi.org/10.1145/1397735.1397744
Krosnick, J. a. (1999). Survey research. *Annual Review of Psychology*. https://doi.org/10.1146/annurev.psych.50.1.537
Kshetri, N. (2014). Big datas impact on privacy, security and consumer welfare. *Telecommunications Policy*, *38*(11), 1134–1145. https://doi.org/10.1016/j.telpol.2014.10.002
Madden, M., Lenhart, A., & Cortesi, S. (2013). Teens, social media, and privacy. *Pew Internet & …*, 107. Retrieved from http://www.lateledipenelope.it/public/52dff2e35b812.pdf
Malhotra, N. K., Kim, S. S., Agarwal, J., Tech, G., & Peachtree, W. (2004). Internet Users ' The Information the Scale , and a Causal (IUIPC): *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.l040.0032
Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. https://doi.org/10.1177/1461444814543995
Metzger, M. J. (2006). Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication*, *9*(4), 00–00. https://doi.org/10.1111/j.1083-6101.2004.tb00292.x
Mislove, A., Viswanath, B., Gummadi, K., & Druschel, P. (2010). You are who you know: inferring user profiles in online social networks. *Third ACM International Conference on Web Search and Data Mining*, 251–260. https://doi.org/10.1145/1718487.1718519

Nagy, J., & Pecho, P. (2009). Social networks security. In *Proceedings - 2009 3rd International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2009* (pp. 321–325). https://doi.org/10.1109/SECURWARE.2009.56

Nentwich, M., & König, R. (2014). Academia Goes Facebook? The Potential of Social Network Sites in the Scholarly Realm, 107–124. https://doi.org/10.1007/978-3-319-00026-8

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

O'Reilly, T. (2006). Web 2.0 Compact definition: trying again. 2006. Retrieved December 29, 2017, from http://radar.oreilly.com/2006/12/web-20-compact-definition-tryi.html

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior*, *50*, 252–258. https://doi.org/10.1016/j.chb.2015.04.011

Raymond, E. S., & Steele, G. L. (1996). *The new hacker's dictionary*. Mit Press.

Ringrose, J., & Harvey, L. (2015). Boobs, back-off, six packs and bits: Mediated body parts, gendered reward, and sexual shame in teens' sexting images. *Continuum*, *29*(2), 205–217. https://doi.org/10.1080/10304312.2015.1022952

Rodrigues, N., & Oliveira, A. (2018). REMEMBER WHEN, ON THE INTERNET, NOBODY KNEW WHO YOU WERE? In *ICERI2018 Proceedings* (pp. 3871–3877). Seville, SPAIN: IATED. https://doi.org/10.21125/iceri.2018.1864

Rosenblum, D. (2007). What anyone can know: The privacy risks of social networking sites. *IEEE Security and Privacy*, *5*(3), 40–49. https://doi.org/10.1109/MSP.2007.75

Rust, R. T., Kannan, P. K., & Peng, N. (2002). The customer economics of internet privacy. *Journal of the Academy of Marketing Science*, *30*(4), 455–464. https://doi.org/10.1177/009207002236917

Sadeghian, A., Zamani, M., & Shanmugam, B. (2013). Security Threats in Online Social Networks. *International Conference on Informatics and Creative Multimedia*, 254–258. https://doi.org/10.1109/ICICM.2013.50

Salomon, D. (2013). Moving on from Facebook: Using Instagram to connect with undergraduates and engage in teaching and learning. *College & Research Libraries News*. https://doi.org/10.5860/crln.74.8.8991

Shapiro, S. S. (2010). Privacy by design. *Communications of the ACM*, *53*(6), 27. https://doi.org/10.1145/1743546.1743559

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

Smith, A., & Anderson, M. (2018). Social Media Use 2018: Demographics and Statistics. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/

Stacey, C. (2017). The Walk of (Body) Shame: The Detrimental Repercussions of Cyberbullying. *The Boller Review*, *2*.

Stieger, S., Burger, C., Bohn, M., & Voracek, M. (2013). Who Commits Virtual Identity Suicide? Differences in Privacy Concerns, Internet Addiction, and Personality Between Facebook Users and Quitters. *Cyberpsychology, Behavior, and Social*

Networking, *16*(9), 629–634. https://doi.org/10.1089/cyber.2012.0323
Taddicken, M. (2014). The "Privacy Paradox" in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. https://doi.org/10.1111/jcc4.12052
Travers, J., & Milgram, S. (1969). An Experimental Study of the Small World Problem. *Sociometry*, *32*(4), 425. https://doi.org/10.2307/2786545
Van Dijk, J. (2012). *The network society*. Sage Publications.
Wellman, B. (2004). The glocal village: Internet and community. *The Arts & Science Review.–University of Toronto*, *1*(1), 26–30. Retrieved from http://www.ideasmag.artsci.utoronto.ca/i/issue1_1/idea_s01-wellman.pdf
Yardley, L. (2017). Demonstrating the validity of qualitative research. *The Journal of Positive Psychology*, *12*(3), 295–296. https://doi.org/10.1080/17439760.2016.1262624
Ybarra, M. L., Boyd, D., Korchmaros, J. D., & Oppenheim, J. (2012). Defining and measuring cyberbullying within the larger context of bullying victimization. *Journal of Adolescent Health*, *51*(1), 53–58. https://doi.org/10.1016/j.jadohealth.2011.12.031
Yenisey, M. M., Ozok, A. A., & Salvendy, G. (2005). Perceived security determinants in e-commerce among Turkish university students. *Behaviour and Information Technology*, *24*(4), 259–274. https://doi.org/10.1080/0144929042000320992
Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, *16*(4), 479–500. https://doi.org/10.1080/1369118X.2013.777757
Zheleva, E., & Getoor, L. (2009). To Join or Not to Join : The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles. *Security*, *7*(1), 531–540. https://doi.org/10.1145/1526709.1526781
Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2014.12.012

Anexos e Apêndices

Anexo A – Artigo em conferência "Remember when, on the Internet, nobody knew who you were?" In ICERI2018 Proceedings

Remember when, on the internet, nobody knew who you were?

Nelson Rodrigues[1], Abílio Oliveira[2]
[1]Instituto Universitário de Lisboa (ISCTE-IUL) (PORTUGAL)
[2]Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR-IUL, Lisboa (PORTUGAL)

Abstract

Social Networking Services have seen an unprecedented adoption rate in the world of information technologies. This adherence has been so strong that even new psychiatric pathologies have been risen around them. Notwithstanding the numerous benefits of using social networking services, these systems live from information share between their users, and very often this information is private. Although social network services have numerous privacy and security settings, and management features, many users choose - consciously or unintentionally - to make excessive or uncontrolled sharing of personal information with social network services. This supposed controlled sharing of personal information on social media can put people at risk, or even in threatening situations, either to the individual himself or to others, linked to his network or family. An exploratory study was conducted through a focus group involving 12 college students attending the first year of an undergraduate program. This study aims, particularly, to understand how college students perceive their own online exposition, and the importance that this has on their privacy and the security of information shared, in social networking services. The data gathered from the focus group was analyzed with an online content analysis software – using the Leximancer platform. From the content analysis of the focus group several important concepts emerged: social network companies, location information, information sharing and distribution, user awareness changes. Findings suggest students are getting a new approach to privacy concerns over social media. Even though they are aware of the risks inherent in over-sharing private data, when faced with "to share or not to share" very often they tend to overlook the privacy concerns in favour of the social exposition. The obtained items and concepts were also used to develop a questionnaire, to be answered by a population of college students, in a subsequent study.

Keywords: Social Networking Services, Social Media, Online privacy, Perceived Privacy, Trust in Social Networking Services, Information Control

1 INTRODUCTION

In 1993 through the hands of an American magazine cartoonist[22] a popular metaphor was born – On the Internet, nobody knows you're a dog – on this cartoon we find two dogs (one of them using a computer) discussing the advantages of Internet and anonymity, this cartoon became a popular symbol for the Internet privacy, something that was implicit in the use of the Internet at the beginning of mainstream Internet. Years later in 2015 we find on the same magazine a new cartoon, featuring a similar pair of dogs watching their owner at a computer, this time one of the dogs asks to the other "Remember when, on the Internet, nobody knew who you were?".

[22] Peter Steiner, cartoonist and contributor to *The New Yorker* since 1979.

These two cartoons pretty much represent the evolution that occurred in the Internet landscape on the last 20 years towards online user's information. This evolution has been based in the continued erosion of privacy, fuelled by a medium where no government intervention is actually effective, leaving privacy at the hands of the free-market forces, enabling the scenario where the amount of privacy online will continue to decline over time and that privacy will be more and more expensive to maintain (Rust, Kannan, & Peng, 2002).

Although it has been increasingly easy for companies and organizations to collect online user's information on their own systems, the peak to user's personal data collection is social networking systems, namely, online social networks. "If you're not paying for it, you became the product" (Goodson, 2012).

Since its beginning social networking services such as Facebook, Twitter, LinkedIn, Pinterest or Instagram, have attracted millions of users. For many people using social networks online, the use of these platforms became part of their daily routines. With the massification of mobile technologies, there has been a growing ubiquity of social networks in people's daily lives. This omnipresence is so intense that in some cases even truly obsessive pathologies can develop [3] [4].

Well since the beginning of the massification of the Internet (1995) it is known that intensive exposure to the world wide web causes the decline of family communication, the reduction of social circle and an increase in depression and loneliness of individuals (Castells, 2002). It is precisely this contraction of the social circle that impels the use of social networks in order to compensate for the social deficit. Social networking sites are excellent means for the development of multiple weak links, in turn these weak ties are great vehicles for obtaining information and opportunities (Castells, 2002).

A social networking site is an Internet-based service that allows people to build public or semi-public profiles, create lists of other users with whom they share a connection, view and cross-check their connection lists with those of other users, all these iterations occur within a limited system (Boyd & Ellison, 2007). Social networking sites are the pinnacle of the "privatization of sociability" (Castells, 2002), that is, they expedite the reconstruction of the social circle through an individual-centred community, as a kind of social geocentrism.

The creation of the first social networking site in 1997, "SixDegrees.com", showed a great desire of people for this type of technology, this led to the appearance of hundreds of social networking sites, which in some cases grew so quickly that they attracted the attention of both the media and academia [6] [7].

Although social networks offer a whole range of interaction opportunities among their users, they also attract the attention of non-users, particularly for issues related to privacy and security. These concerns can be effectively substantiated, however, social networking sites have long since ceased to be niche phenomena (Gross & Acquisti, 2005), millions of people around the world consciously and voluntarily use these social networks to communicate, find friends, make appointments and look for jobs. By doing all these activities, they deliberately reveal highly personal information not only to acquaintances but also to strangers - for example - birth dates, mobile phone numbers or the current address are common data in social networks [9] [10].

We cannot but marvel with the nature, quantity and detail of personal information that some users provide, at the same time we must consider how informed this information sharing is (Gross & Acquisti, 2005). There is a low awareness of users on how to protect their personal information on social networks (Nagy & Pecho, 2009) and do not always have a clear idea about who has access to it or how it can be used (Krishnamurthy & Wills, 2008).

More than 40% of social network users share private information (Hajli & Lin, 2016), this information may be shared and used without the express consent of the owner, making users vulnerable to various online threats such as fraud, identity theft, phishing, among others. Once information is placed on a social network, it ceases to be effectively private (Sadeghian et al., 2013).

Having already registered growth rates of 3% per week (Bilge et al., 2009) and being the largest repository of photos on the Internet, Facebook is undoubtedly the *de facto* social network, this hegemony of Facebook also increases its attractiveness to criminals, having arisen several pieces of software capable of launching automated attacks that allow identity theft or profile cloning (Bilge et al., 2009).

In addition to personal information, social networks also allow the sharing of content, knowledge and experiences. This personally identifiable information can also quickly feed the profile design or serve as critical mass for commercial or political purposes without the users' knowledge.

Having a private and secure profile seems like a good idea for more conscientious users, but their connections with others and affiliations with public groups can also pose a threat to their security, as it is possible to exploit social networks to predict personal and sensitive information based on public information (Kosinski et al., 2013; Mislove, Viswanath, Gummadi, & Druschel, 2010; Zheleva & Getoor, 2009).

Simultaneously with the unbeatable growth of social networking sites and growing security concerns arising from its use, we need to add to this mixture the mobile devices, which, with new technologies, create additional security and privacy problems when collecting and making available the users' private information in social networks, specifically the geographical location (Kizza, 2001).

According to Shin (Shin, 2010) the attitude of users towards social networks rests on three pillars:

- Security: User perception of security, defined by the extent to which a user believes that using a system will be risk-free.
- Privacy: Control of the flow of personal information, including the transfer and exchange of this information.
- Trust: Social network trust is defined as the user's willingness to be vulnerable to the actions of the social network system, based on the expectation that the social network system will perform a particular action important to the user, regardless of the user's ability to monitor the social networking system.

2 METHODOLOGY

The main goal for this research is to understand the perceptions on privacy, self-exposition and social network services on college students. This has been achieved through seven components: the perception of privacy; the perception of security; the trust relationship with the social network services; awareness (of privacy practices); data collection recognition; identification of unauthorized secondary use; the perception of risks.

We conducted an exploratory study using a focus group composed of 12 college students attending the first year of an undergraduate program. The gender distribution was 17% male and 83% female, the age interval was between 19 and 26 years. The students were informed that their participation in the study was voluntary and that no private or personal information was to be collected.

The choice of focus group as the instrument for this study showed to be the best approach for generating concepts, usually elusive in regular questionnaires (Kitzinger, 1994). The focus group was conducted through a semi-structured interview, below you can find some of the questions asked to the panel:

- Do you think the Internet poses privacy issues? What about social networks? What kind of problems?
- Is it safe to think that the information provided to social networking sites will not be changed by third parties?
- Are social media sites honest with users?
- Advertising a clear online privacy policy is important to make users aware? Why?
- Does the collection of personal information by social networking sites upset you?
- Do you think social networking sites market user data to other companies?
- Is it risky to provide private/personal information on social networking sites? Why?

The plan was to raise several themes and see how the different concepts were approached and related. Data gathered from the answers was then analyzed through Leximancer online platform, which is a text mining software used to extract meaningful concepts from non-structured textual content. Leximancer digests the text to find all possible concepts, then, we analyze and remove all concepts not significant for each question. We managed Leximancer to produce a graphic that links all the concepts.

3 RESULTS

Perceptions on privacy and self-exposition in social network services of college students

On the following graphic (see Figure 1) we can see a whole realm of concepts that emerged from our focus group. Through the exploration of these concepts we reach some results, next, we present the interpretation of the data obtained supported by extracts from the answers.

Users turn to social networks because they exist and know that this has a certain meaning for them as users, they know the kind of social networks that exist and know what is associated with them, they have that notion. This implies, if they know what it is, and have a sense of what social networks are, we already know why they go there, they go to: talk, publicize, participate in events, groups and chats, make comments, laugh, cry. In sum to disclose what they should and should not do (Acquisti & Gross, 2006; Boyd, 2008, 2014; Ellison & Boyd, 2013; Hallam & Zanella, 2017).

The concept "users" has an intersection with social networks, whereas the concept of companies does not, this might mean that users are "inside" social networks, they are closer to social networks, in extreme one could say they are the social networks, we thus see a merger between the social life and digital life of users (Ellison et al., 2007; Rosenblum, 2007). In short, users know what social networks are, but they get and stay onboard anyway.

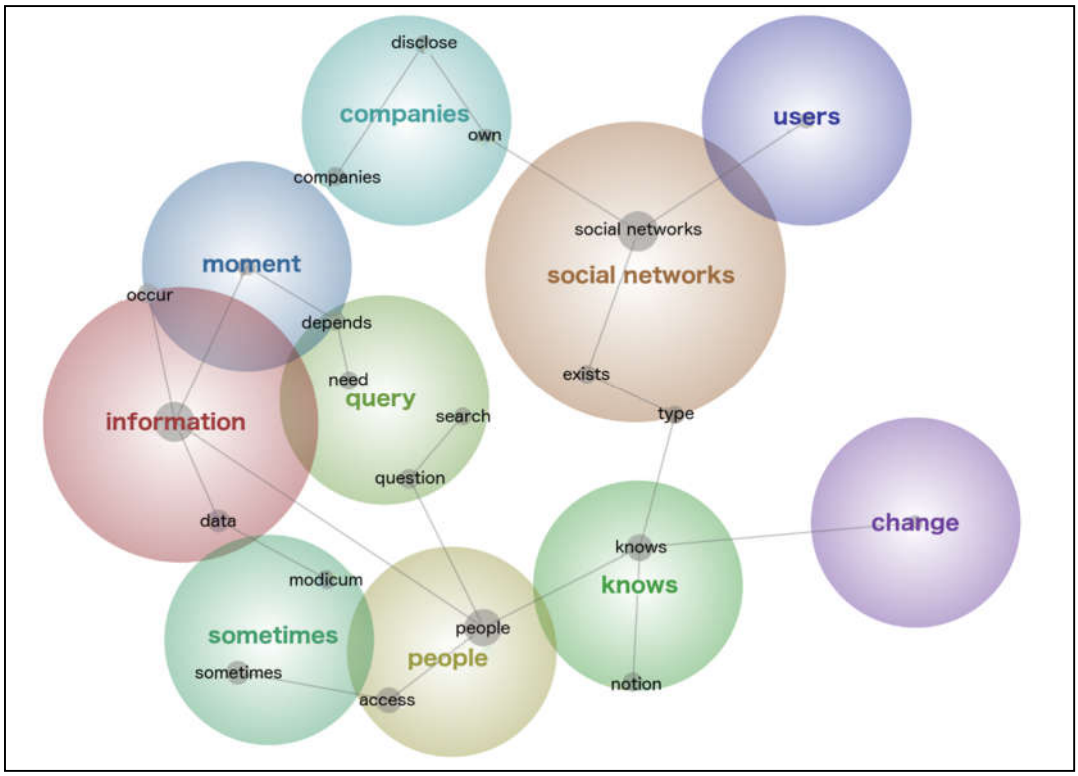

Figure 1. Analysis / Perception of privacy, self-exposition and social network services on college students

On the other hand, companies use social networks to publicize their own initiatives, always in their own interest. The concept "companies" does not interconnect with social networks, there is a gap, companies only use social networks, they are not part of it. Observe that users are also not connected to anything else other than social networks, so the concept of social networks is what connects users to companies. From the point of view of the companies this is excellent, they manage to capture the attention of users. From the point of view of users, it's the usual story "I do not disclose anything, but everybody knows everything about me" [26] [27].

People know what social networks are and have a notion about it, funny that at the same time, there is here a notion of change, that is, we are facing a possible change in the notion (perception) of what is a social network, we are faced with a process of external change. Note that it is not in the users of social networks that this change is observed, it is in people. This shows a latent disassociation between the concepts user and person.

From the point of view of people, we see that sometimes they access social networks and in part they go there to seek information. People use social networks basically for queries, to look for information, but only sometimes, the rest of the time people produce information, this information can be text, images, videos, location information, etc...

On the one hand, people know that they can change and that they can somehow also cultivate their privacy, but on the other hand, they basically use social networks to exchange information. We are dealing here with a paradox (Barnes, 2006), to what extent do people have the notion that by exchanging so much information they even know they can change. Do they really know they can change their privacy issues, their behavior and the way they react? In some way it is a kind of giving up, it's almost like a feeling of apathy towards privacy [29] [30].

'… we are not going to change our habits even knowing that, therefore, this (privacy concerns) exist, we continue to live on the bubble and we accept that …';

'… but there it is, if we think too much of course it concerns, but it is the question of conscious naivete, we do know the risks, but maybe we do not care so much …'.
Another concept emerges, interacting on social networks is a matter of the moment, people can do something at a specific moment in time, yet for sharing something at that particularly moment the person might keep thinking about the consequences that it will have:
'… sometimes I do not share certain things (online) because I get that feeling in the subconscious and think that maybe they might be used against me, so I do not share so many things, but also it depends on the moment and place, there are times when we are doing things that we are so enthusiastic about what we are doing that we share without thinking …';
'This is going to have other repercussions, for example we are now in college, but when we go to the job market, if the recruiting companies want they can do an investigation on us, and almost surely will find quite embarrassing things about us …'.
There is this idea that what is lived at the present moment has already passed, and that in a way already belongs to the past, the problem is that it does not go away, it gets recorded in the social networks for future reference, and it will be recalled, eventually out of the initial context (Rosenblum, 2007). This moment depends on the need to look for questions, these questions can be affective or social, and as we see a bond between queries and information basically people are sharing and looking for everything that has to do with their personal life [23] [32].
On the graphic we do not find any privacy concepts, but it is quite relevant the focus attributed to the information concept (2nd largest dimension) it is because in fact students may even think that privacy is an important thing, but once they enter the social networks they forget about it.
Companies are between social networks and the moment, companies clearly take advantage of the moment, realizing the huge role of social networks helping them spread what they do, assume here a commercial role, taking advantage of the moments that people are living to exhibit what they do and at the same time get access to the information that users put on social networks.
It is curious that when the person puts himself in the role of the user his behavior changes, "one thing is what I do as a user, another thing is what people do". People in general live the moments, look for various questions, share information, but they know what social networks are, notice that they know that at any time they can change. This dichotomy user *versus* person, is if the user and the person are two different things, this is to say, the privacy attitude and the privacy behavior are two different things (Kokolakis, 2017). This dichotomy is enhanced by the notion of the present moment, students tend to overestimate the present benefit of sharing information against the eventual future loss of privacy (Hallam & Zanella, 2017).
'… these people think that only what they put on the Net is going to appear, I think these people do not have this notion well …';
'… I think there are people who think that just for example, Google has access to the data, they think it's just the phone that has the data and only there because it opened the application…';
'… I have Facebook because there is no Messenger, and I have WhatsApp because it's the thing that my group at the University uses to communicate, as far as I'm concerned I would not use any of these social networks, I do not care, I don't even publish anything …'.

4 CONCLUSIONS

After the recent events of personal data breach that happened on Facebook, whose most popular is undoubtedly the Cambridge Analytica scandal (Greenfield, 2018), which exposed some serious implications that can happen over private/personal information gathered from social networks, this kind of work is increasingly urgent to spread and sensitize the community in general and academia in particular to the potential dangers of the invasion of social networks in the sphere of each citizen's own private life.

From our analysis to all the concepts about privacy and social networks that emerged from our focus group with college students, several conclusions can be made. First of all, what ties companies and users together are social networks, people know what a social network is and what type of social networks there are, there is even a change possibility in the horizon for new privacy behaviours to start happening. Meanwhile people are sharing and collecting information of their moments and their social network moments. These moments in time are faced as belonging to the distant past, almost as disappeared. Although there is an increasingly concern for the future usage of this information, that it might create difficulties and constraints on the next stage of college students when they start entering the job market.

Finally, our focus group evidenced the discrepancy that exists between the role of the user of social networks from the role of people as information providers and consumers, they both are perceived as distinct beings, it's a typical "us and them", although evidently all users are in fact people.

Following this work, a questionnaire will be developed, and these findings should be confirmed with a subsequent inferential study.

ACKNOWLEDGEMENTS

The authors would like to express their gratitude to Ana Filipa Rodrigues and Sara Bonifácio for their invaluable assistance making possible the focus group.

REFERENCES

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the facebook. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 4258 LNCS, pp. 36–58). https://doi.org/10.1007/11957454_3

Ahn, G.-J., Shehab, M., & Squicciarini, A. (2011). Security and Privacy in Social Networks. *IEEE Internet Computing*, *15*(3), 10–12. https://doi.org/10.1109/MIC.2011.66

Aldhafferi, N., Watson, C., & A.S.M, S. (2013). Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices. *International Journal of Security, Privacy and Trust Management*, *2*(2), 1–17. https://doi.org/10.5121/ijsptm.2013.2201

Andreassen, C. S., Torsheim, T., Brunborg, G. S., & Pallesen, S. (2012). Development of a Facebook Addiction Scale. *Psychological Reports*, *110*(2), 501–517. https://doi.org/10.2466/02.09.18.PR0.110.2.501-517

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9), 5. https://doi.org/10.5210/fm.v11i9.1394

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2015.07.025

Bilge, L., Strufe, T., Balzarotti, D., Kirda, E., & Antipolis, S. (2009). All Your Contacts Are Belong to Us : Automated Identity Theft Attacks on Social Networks. *Www 2009*, 551–560. https://doi.org/http://doi.acm.org/10.1145/1526709.1526784

Bonneau, J., & Preibusch, S. (2010). The privacy jungle: On the market for data

protection in social networks. *Economics of Information Security and Privacy*, 1–45. https://doi.org/10.1007/978-1-4419-6967-5_8

Boyd, D. (2008). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *Convergence*, *14*(1), 13–20. https://doi.org/10.1177/1354856507084416

Boyd, D. (2014). *It's Complicated: The Social Lives of Networked Teens*. *It'S Complicated: the Social Lives of Networked Teens*. Yale University Press. https://doi.org/10.1007/s10615-014-0512-3

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

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, *15*(8). https://doi.org/10.5210/fm.v15i8.3086

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 154–165. https://doi.org/10.1002/asi.20459

Castells, M. (1996). *The Rise of the Network Society. The Information Age: Economy, Society, and Culture Volume I (Information Age Series)*. London: Blackwell.

Castells, M. (2002). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford University Press on Demand.

Cavoukian, A. (2011). Privacy by Design. *The 7 Foundational Principles*, 1–2. Retrieved from http://publication/uuid/9F8761B1-D114-42A3-9AF0-4521C5D78F2A

Cecere, G., Le Guel, F., & Soulié, N. (2015). Perceived Internet privacy concerns on social networks in Europe. *Technological Forecasting and Social Change*, *96*, 277–287. https://doi.org/10.1016/j.techfore.2015.01.021

Chen, H.-T., & Chen, W. (2015). Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 13–19. https://doi.org/10.1089/cyber.2014.0456

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*. https://doi.org/10.1002/ejsp.2049

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Americas Conference on Information Systems (AMCIS)*, *123*, 339–350. https://doi.org/10.1.1.148.9388

Ellison, N. B., & Boyd, D. (2013). Sociality through social network sites. *The Oxford Handbook of Internet Studies*, 151–172. https://doi.org/10.1093/oxfordhb/9780199589074.001.0001

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, *12*(4), 1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. https://doi.org/10.1016/j.chb.2008.08.006

Freitas, H., Oliveira, M., Jenkins, M., & Popjoy, O. (1998). The Focus Group, A Qualitative Research Method. *Isrc*, (010298), 1–22. https://doi.org/10.1016/j.watres.2013.02.032

Goodson, S. (2012). If You're Not Paying For It, You Become The Product.
Greenfield, P. (2018). The Cambridge Analytica files: the story so far. *The Guardian*.
Gressin, S. (2017). The Equifax data beach: What to do. *Federal Trade Commission*, (September), 8–10. Retrieved from https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do
Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Privacy in the Electronic Society 2005*, 11. https://doi.org/10.1145/1102199.1102214
Guha, S., Tang, K., & Francis, P. (2008). NOYB: Privacy in Online Social Networks. *Proceedings of the First Workshop on Online Social Networks*, 49–54. https://doi.org/http://doi.acm.org/10.1145/1397735.1397747
Hajli, N., & Lin, X. (2016). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics*, *133*(1), 111–123. https://doi.org/10.1007/s10551-014-2346-x
Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2016.11.033
Hargittai, E. (2010). Digital Na(t)ives? Variation in internet skills and uses among members of the "net Generation." *Sociological Inquiry*, *80*(1), 92–113. https://doi.org/10.1111/j.1475-682X.2009.00317.x
Hargittai, E., & Marwick, A. (2016). "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication*, *10*(0), 21.
Haridakis, P., & Hanson, G. (2009). Social interaction and co-viewing with YouTube: Blending mass communication reception and social connection. *Journal of Broadcasting and Electronic Media*. https://doi.org/10.1080/08838150902908270
Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic Commerce Research and Applications*, *9*(1), 50–60. https://doi.org/10.1016/j.elerap.2009.05.001
Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59–68. https://doi.org/10.1016/j.bushor.2009.09.003
Kaufman, L. (2009). Data security in the world of cloud computing, security and privacy. *Ieee*, *7*(4), 61–64.
Kitzinger, J. (1994). The methodology of Focus Groups: the importance of interaction between research participants. *Sociology of Health & Illness*, *16*(1), 103–121. https://doi.org/10.1111/1467-9566.ep11347023
Kitzinger, J. (1995). Introducing focus groups ' P. *BMJ : British Medical Journal*, *311*, 299–302.
Kizza, J. M. (2001). *Computer network security and cyber ethics*. McFarland.
Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*. https://doi.org/10.1016/j.cose.2015.07.002
Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110
Krasnova, H., Kolesnikova, E., Guenther, O., & Günther, O. (2009). "It Won't Happen To Me!": Self-Disclosure in Online Social Networks. *Amcis 2009 Proceedings*, 343. https://doi.org/10.7892/boris.47460

Krishnamurthy, B., & Wills, C. E. (2008). Characterizing privacy in online social networks. *Proceedings of the First Workshop on Online Social Networks (WOSP '08)*, 37–42. https://doi.org/10.1145/1397735.1397744

Krosnick, J. a. (1999). Survey research. *Annual Review of Psychology*. https://doi.org/10.1146/annurev.psych.50.1.537

Kshetri, N. (2014). Big datas impact on privacy, security and consumer welfare. *Telecommunications Policy*, *38*(11), 1134–1145. https://doi.org/10.1016/j.telpol.2014.10.002

Madden, M., Lenhart, A., & Cortesi, S. (2013). Teens, social media, and privacy. *Pew Internet & …*, 107. Retrieved from http://www.lateledipenelope.it/public/52dff2e35b812.pdf

Malhotra, N. K., Kim, S. S., Agarwal, J., Tech, G., & Peachtree, W. (2004). Internet Users ' The Information the Scale , and a Causal (IUIPC): *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.l040.0032

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. https://doi.org/10.1177/1461444814543995

Metzger, M. J. (2006). Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication*, *9*(4), 00–00. https://doi.org/10.1111/j.1083-6101.2004.tb00292.x

Mislove, A., Viswanath, B., Gummadi, K., & Druschel, P. (2010). You are who you know: inferring user profiles in online social networks. *Third ACM International Conference on Web Search and Data Mining*, 251–260. https://doi.org/10.1145/1718487.1718519

Nagy, J., & Pecho, P. (2009). Social networks security. In *Proceedings - 2009 3rd International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2009* (pp. 321–325). https://doi.org/10.1109/SECURWARE.2009.56

Nentwich, M., & König, R. (2014). Academia Goes Facebook? The Potential of Social Network Sites in the Scholarly Realm, 107–124. https://doi.org/10.1007/978-3-319-00026-8

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

O'Reilly, T. (2006). Web 2.0 Compact definition: trying again. 2006. Retrieved December 29, 2017, from http://radar.oreilly.com/2006/12/web-20-compact-definition-tryi.html

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior*, *50*, 252–258. https://doi.org/10.1016/j.chb.2015.04.011

Raymond, E. S., & Steele, G. L. (1996). *The new hacker's dictionary*. Mit Press.

Ringrose, J., & Harvey, L. (2015). Boobs, back-off, six packs and bits: Mediated body parts, gendered reward, and sexual shame in teens' sexting images. *Continuum*, *29*(2), 205–217. https://doi.org/10.1080/10304312.2015.1022952

Rodrigues, N., & Oliveira, A. (2018). REMEMBER WHEN, ON THE INTERNET, NOBODY KNEW WHO YOU WERE? In *ICERI2018 Proceedings* (pp. 3871–3877). Seville, SPAIN: IATED. https://doi.org/10.21125/iceri.2018.1864

Rosenblum, D. (2007). What anyone can know: The privacy risks of social networking

sites. *IEEE Security and Privacy*, *5*(3), 40–49. https://doi.org/10.1109/MSP.2007.75

Rust, R. T., Kannan, P. K., & Peng, N. (2002). The customer economics of internet privacy. *Journal of the Academy of Marketing Science*, *30*(4), 455–464. https://doi.org/10.1177/009207002236917

Sadeghian, A., Zamani, M., & Shanmugam, B. (2013). Security Threats in Online Social Networks. *International Conference on Informatics and Creative Multimedia*, 254–258. https://doi.org/10.1109/ICICM.2013.50

Salomon, D. (2013). Moving on from Facebook: Using Instagram to connect with undergraduates and engage in teaching and learning. *College & Research Libraries News*. https://doi.org/10.5860/crln.74.8.8991

Shapiro, S. S. (2010). Privacy by design. *Communications of the ACM*, *53*(6), 27. https://doi.org/10.1145/1743546.1743559

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

Smith, A., & Anderson, M. (2018). Social Media Use 2018: Demographics and Statistics. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/

Stacey, C. (2017). The Walk of (Body) Shame: The Detrimental Repercussions of Cyberbullying. *The Boller Review*, *2*.

Stieger, S., Burger, C., Bohn, M., & Voracek, M. (2013). Who Commits Virtual Identity Suicide? Differences in Privacy Concerns, Internet Addiction, and Personality Between Facebook Users and Quitters. *Cyberpsychology, Behavior, and Social Networking*, *16*(9), 629–634. https://doi.org/10.1089/cyber.2012.0323

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

Travers, J., & Milgram, S. (1969). An Experimental Study of the Small World Problem. *Sociometry*, *32*(4), 425. https://doi.org/10.2307/2786545

Van Dijk, J. (2012). *The network society*. Sage Publications.

Wellman, B. (2004). The glocal village: Internet and community. *The Arts & Science Review.–University of Toronto*, *1*(1), 26–30. Retrieved from http://www.ideasmag.artsci.utoronto.ca/i/issue1_1/idea_s01-wellman.pdf

Yardley, L. (2017). Demonstrating the validity of qualitative research. *The Journal of Positive Psychology*, *12*(3), 295–296. https://doi.org/10.1080/17439760.2016.1262624

Ybarra, M. L., Boyd, D., Korchmaros, J. D., & Oppenheim, J. (2012). Defining and measuring cyberbullying within the larger context of bullying victimization. *Journal of Adolescent Health*, *51*(1), 53–58. https://doi.org/10.1016/j.jadohealth.2011.12.031

Yenisey, M. M., Ozok, A. A., & Salvendy, G. (2005). Perceived security determinants in e-commerce among Turkish university students. *Behaviour and Information Technology*, *24*(4), 259–274. https://doi.org/10.1080/0144929042000320992

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, *16*(4), 479–500. https://doi.org/10.1080/1369118X.2013.777757

Zheleva, E., & Getoor, L. (2009). To Join or Not to Join : The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles. *Security*, *7*(1), 531–

540. https://doi.org/10.1145/1526709.1526781
Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2014.12.012

Apêndice A – Guião Focus Group

Guião para Focus Group em torno do tema: Como percecionamos a nossa exposição e da privacidade nas redes sociais

Introdução: Olá e bem-vindos a este grupo de discussão. O meu nome é Nelson Rodrigues e estou aqui como facilitador/moderador. Estou a trabalhar numa pesquisa no ISCTE-IUL sobre a Perceção da exposição pessoal e da privacidade nas redes sociais entre estudantes universitários. O meu papel é suscitar uma conversa estimulante que abranja uma série de tópicos importantes sobre os quais gostaria de ouvir as vossas opiniões e sugestões.

Objetivo: Em primeiro lugar, agradeço a todos por aqui estarem e se disporem a discutir as vossas ideias. O objetivo desta reunião é compreender as expectativas e recolher opiniões relativamente a à perceção dos estudantes universitários da sua exposição nas redes sociais e a sua privacidade online.

Os objetivos em particular deste estudo são:

- Quais as preocupações dos estudantes universitários com a sua privacidade online.
- Que importância dão à sua exposição online relativamente à sua privacidade e segurança.

Propósito: Explicando o propósito da configuração da reunião do focus group:

- Vós sois a população alvo deste estudo e estou aqui para aprender convosco.
- A vossa participação é voluntária e confidencial.
- Solicito a vossa autorização para gravar em áudio a discussão que se segue, para não se perder nada importante, ao analisar em detalhe todas as informações aqui coligidas unicamente para fins científicos.

Duração: O período total de tempo da reunião do focus group deverá ser aproximadamente 60 minutos.

Regras: No que diz respeito ao focus group, existem algumas "regras básicas":

- Para mantermos a duração do focus group, perguntas ou comentários fora do tópico poderão ser guardados para após a sessão.
- Não existem respostas corretas ou erradas e é suposto existirem opiniões divergentes.
- De forma a preservar a confidencialidade do trabalho peço-vos para tentarem não usar nomes ou outros dados que vos possam identificar diretamente.

Questões:

Perceção de privacidade:

Q1: Estarão os utilizadores cientes das informações que são coletadas por terceiros quando usam sites de redes sociais?

Q2: Que opinião têm sobre esta recolha de dados por entidades externas nas redes sociais?

Q3: Acham que a Internet coloca problemas ao nível de privacidade? E as redes sociais? Que tipo de problemas?

Perceção de segurança:

Q4: Que opinião têm sobre a ideia que os utilizadores fazem da segurança dos seus dados nas redes sociais?
Q5: É seguro pensar que as informações fornecidas aos sites de rede sociais não serão alteradas por terceiros?
Q6: As informações (privadas) que (directa ou indiretamente) damos/publicamos aos/nos sites de redes sociais ficarão seguras?
Q7: Poderão terceiras entidades ver as informações privadas fornecidas aos sites de redes sociais?

Confiança:
Q8: Podemos contar com os sites de redes sociais para proteger a nossa privacidade?
Q9: Os sites de redes sociais são honestos com os utilizadores?

Esfera do controlo:
Q10: A gestão da informação nas redes sociais é o principal fator para garantir a privacidade?

Consciencialização (das práticas de privacidade):
Q11: Pensam que serviços que procuram informação online deveriam divulgar a forma como coletam, processam e usam essa informação?
Q12: Divulgar uma política de privacidade on-line clara é importante para consciencializar os utilizadores? Porquê?

Recolha:
Q13: A recolha de informação pessoal por parte dos sites de redes sociais incomoda-o(a)?
Q14: O fornecimento de informação pessoal nas redes sociais pode ser uma barreira ao uso destes sites?

Uso secundário não autorizado:
Q15: Acha que os sites de redes sociais comercializam os dados obtidos sobre os utilizadores a outras empresas?
Q16: A publicidade direcionada nas redes sociais põe em risco a privacidade dos utilizadores?

Perceção Riscos:
Q17: Será arriscado fornecer informação privada/pessoal nos sites de redes sociais? Porquê?

Fim: Saúdo-vos por esta interessante discussão. Agradeço-vos por terem disponibilizado o vosso tempo, e pelas vossas opiniões sinceras – foi para nós extremamente útil e muito importante.

Novamente, muito obrigado pela vossa participação hoje.

Apêndice B – Guião de Entrevistas

Guião para Entrevistas em torno do tema: A perceção da exposição e da privacidade nas redes sociais

Introdução: O meu nome é Nelson Rodrigues estou a trabalhar num estudo de pesquisa no ISCTE sobre a Perceção da exposição pessoal e da privacidade nas redes sociais entre estudantes universitários.

Objetivo: Em primeiro lugar, agradeço pelo seu tempo para partilhar as suas ideias. O objetivo desta reunião é abordar o tema da perceção da exposição e da privacidade nas redes sociais online. A análise qualitativa desta entrevista irá permitir a sintetizar questões que farão parte de um questionário a difundir junto da comunidade académica discente com vista a atingir os objetivos deste estudo.

Os objetivos em particular deste estudo são:

- Saber como é que os estudantes universitários percecionam as redes sociais e aquilo que expõem online, através dos seus comportamentos, opiniões e partilhas.
- Saber como é que estes representam, a importância desta exposição na sua esfera de privacidade e segurança.
- Compreender como é que os estudantes universitários percecionam o modo como se expõem online e a importância que isso tem na sua privacidade e na segurança da informação partilhada nas redes sociais.

Propósito: Explicando o propósito da entrevista:

- Vós sois o especialista e estou aqui para aprender convosco.
- Isto é estritamente voluntário.
- Solicito a autorização para gravar em áudio a entrevista, para não se perder nada importante, ao analisar em detalhe todas as informações aqui coligidas.

Duração: O período total de tempo da entrevista deverá ser aproximadamente 60 minutos.

Questões:

Perceção de privacidade:

Q1: Estarão os utilizadores cientes das informações que são coletadas por terceiros quando usam sites de redes sociais?

Q2: Acha que os utilizadores sabem a natureza exata das informações que são coletadas durante o uso de sites de redes sociais?

Q3: Pensa que os utilizadores se preocupam que a informação que partilham nos sites de redes sociais possa ser mal utilizada?

Q4: Existem mecanismos eficazes para resolver qualquer violação das informações fornecidas nos sites de rede sociais?

Q5: Acha que a Internet coloca problemas ao nível da privacidade? E as redes sociais? Que tipo de problemas?

Perceção de segurança:

Q6: Que ideia acha que os utilizadores têm da segurança dos seus dados nas redes sociais?
Q7: É seguro pensar que as informações fornecidas aos sites de rede sociais serão alteradas por terceiros?
Q8: É ingenuidade ou indiferença confiar que as informações privadas fornecidas aos sites de redes sociais ficarão seguras?

Confiança:
Q9: Os sites de redes sociais são redes sociais confiáveis?
Q10: Podemos contar com os sites de redes sociais para proteger a privacidade dos seus utilizadores?
Q11: Podem os sites de redes sociais ser convocados a manter as suas garantias expostas nas políticas de privacidade?
Q12: Os sites de redes sociais são honestos com os utilizadores?

Atitude perante os sites de redes sociais:
Q13: A presença de sentimentos positivos em relação aos sites de redes sociais afeta positivamente a perceção de privacidade e segurança das mesmas?

Esfera do controlo:
Q14: A privacidade online é na realidade uma questão do direito de exercer controle e autonomia sobre as decisões de como a informação do utilizador é coletada, usada e compartilhada. Concorda com esta afirmação?
Q15: A possibilidade de controlo de informação pessoal é o cerne da privacidade?

Consciencialização (das práticas de privacidade):
Q16: Pensa que serviços que procuram informação online deveriam divulgar a forma como coletam, processam e usam essa informação?
Q17: Ter uma política de privacidade on-line clara é importante para consciencializar os utilizadores? Porquê?
Q18: É muito importante para os utilizadores terem a noção e o conhecimento sobre como informação pessoal será usada?

Recolha:
Q19: O fornecimento de informação pessoal nas redes sociais pode ser uma barreira ao uso destes sites?

Uso secundário não autorizado:
Q20: O uso da informação pessoal para qualquer tipo de propósito deveria ser explicitamente autorizado pelos utilizadores, concorda?
Q21: Acha que os sites de redes sociais comercializam os dados obtidos sobre os utilizadores a outras empresas?
Q22: A publicidade direcionada e o *profiling* praticados nas redes sociais põe em risco a privacidade dos utilizadores?

Perceção Riscos:
Q23: Será arriscado fornecer informação nos sites de redes sociais? Porquê?
Q24: Acha que existe potencial para a fuga de informação nos sites de redes sociais?

Fim: Acho que chegamos ao fim das perguntas. Deixe-me desde já agradecer o seu contributo e por ter disponibilizado o seu tempo - foi extremamente útil neste estágio ainda inicial deste estudo, mas muito importante.

Novamente, muito obrigado pela sua colaboração hoje.

Apêndice C – Gráficos individuais de componentes do estudo qualitativo

Gráficos de análise aos componentes essenciais obtidos no *Focus Group*

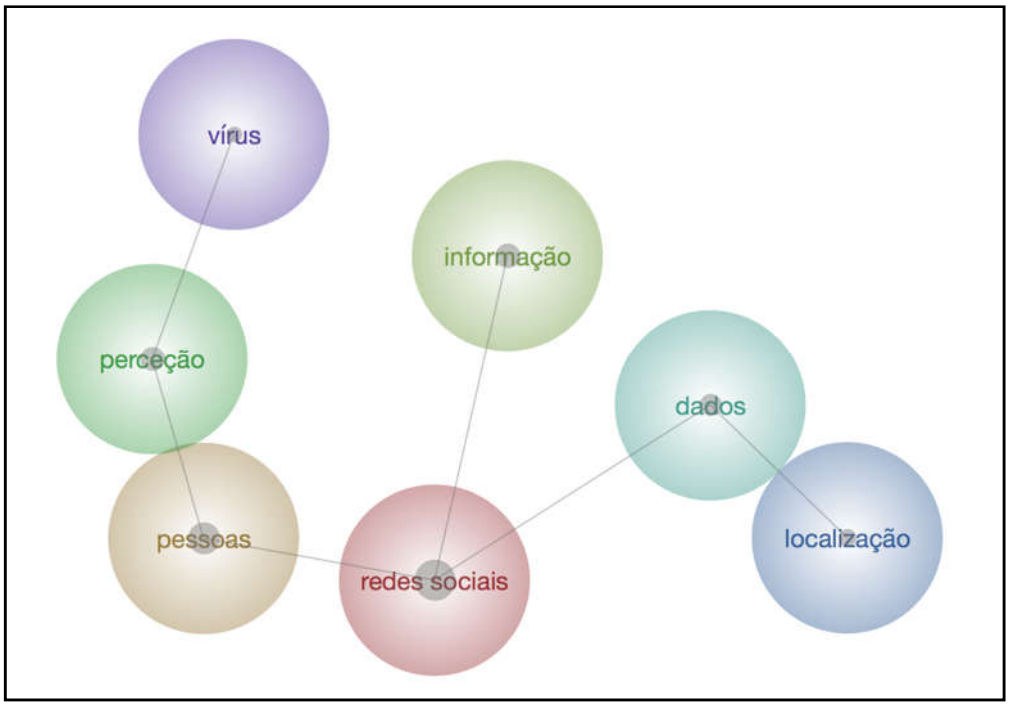

Figura 15 - Focus group – Privacidade

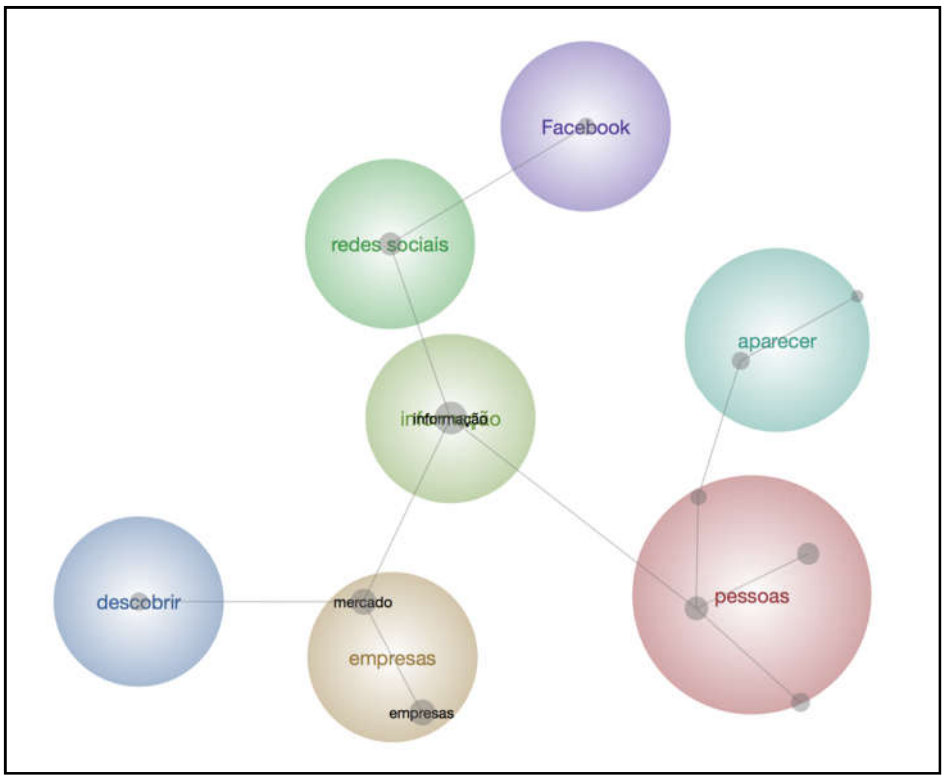

Figura 16 - Focus group – Segurança

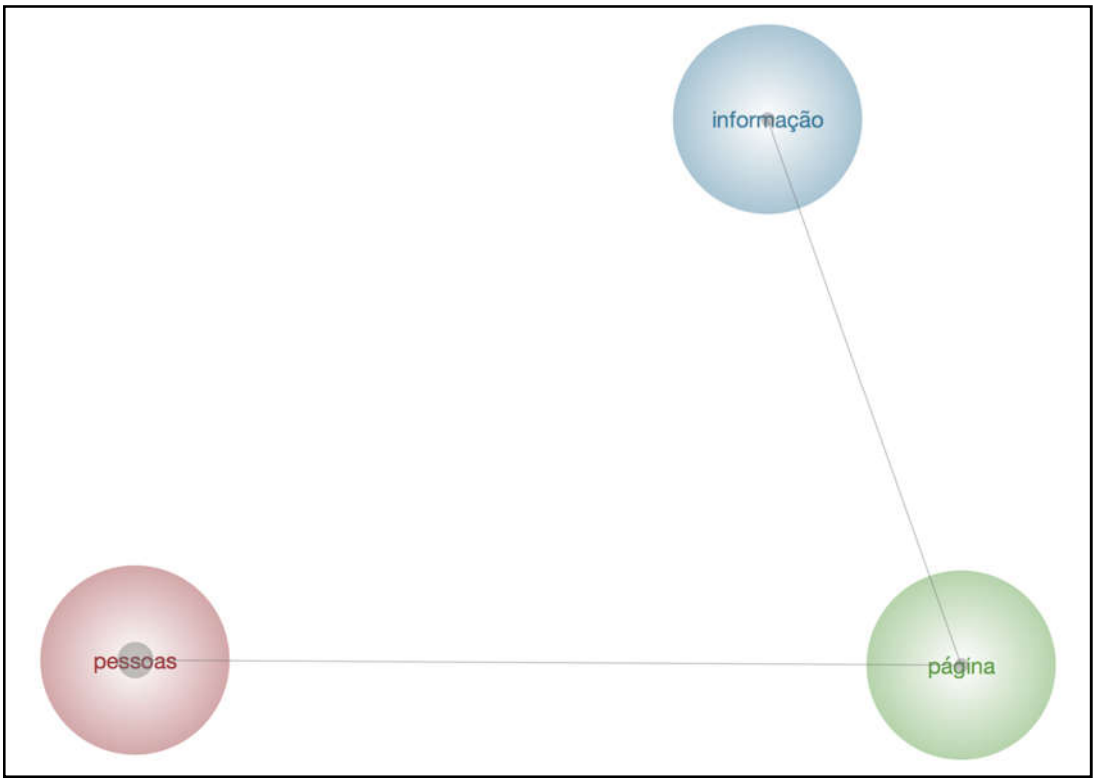

Figura 17 - Focus group – Confiança

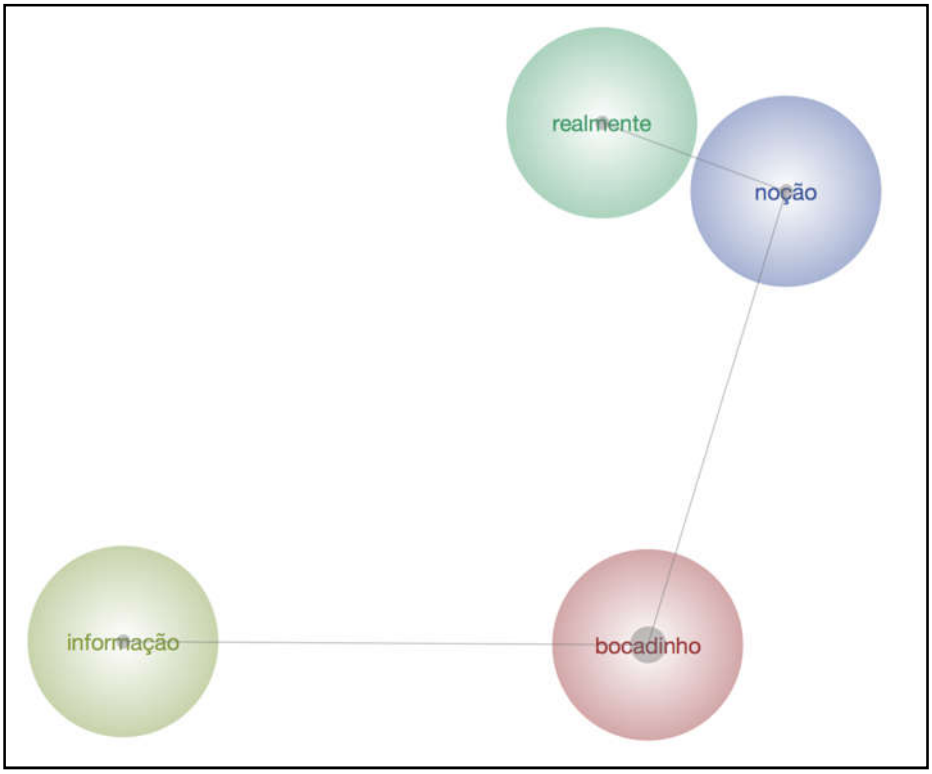

Figura 18 - Focus group – Consciência

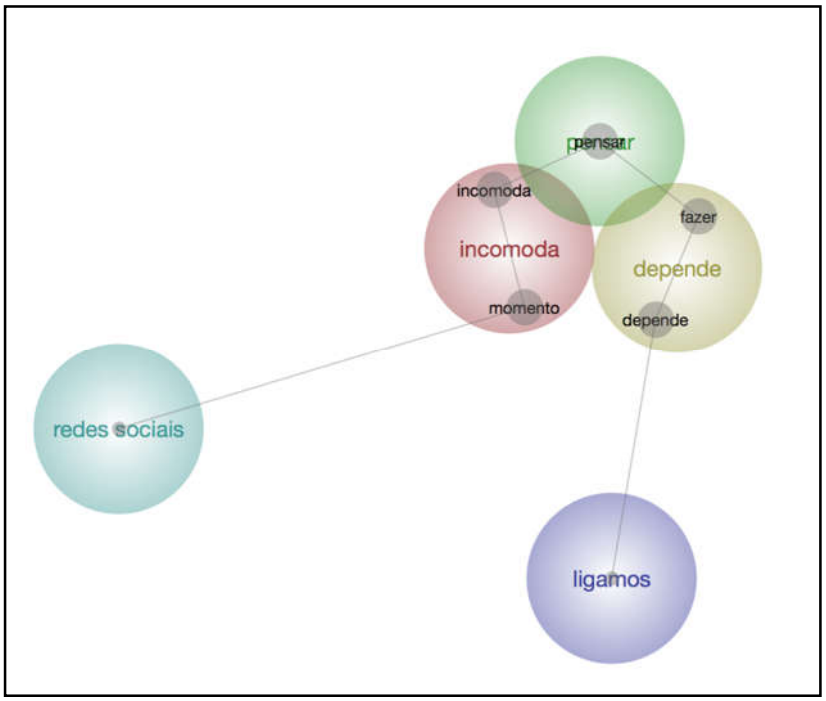

Figura 19 - Focus group – Recolha

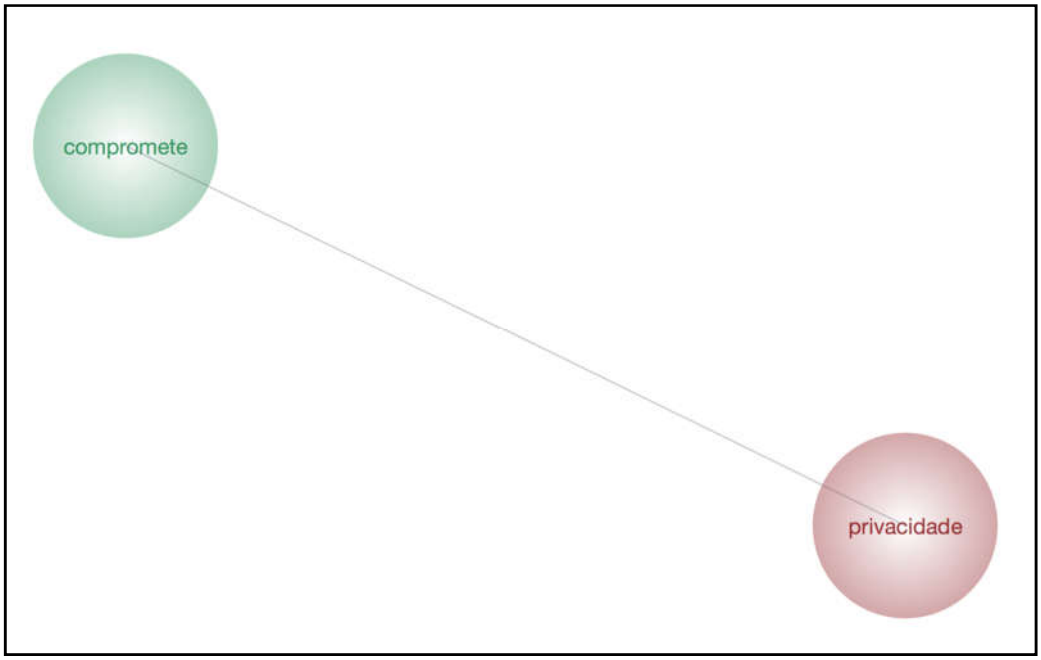

Figura 20 - Focus group - Uso secundário

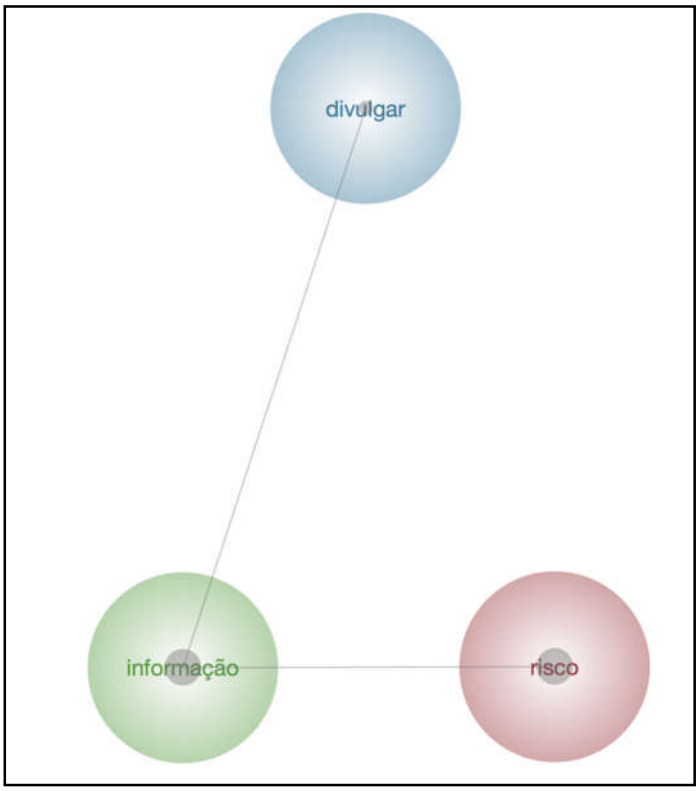

Figura 21 - Focus group - Riscos

Gráficos de análise aos componentes essenciais obtidos nas Entrevistas

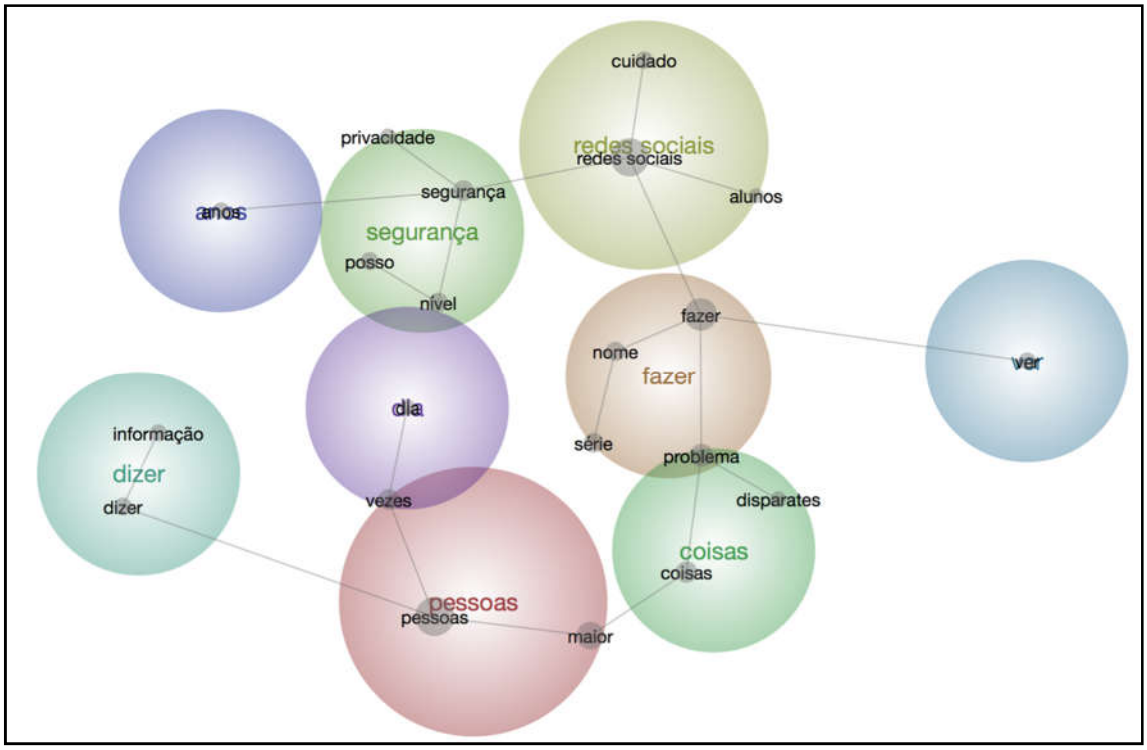

Figura 22 - Entrevistas – Privacidade

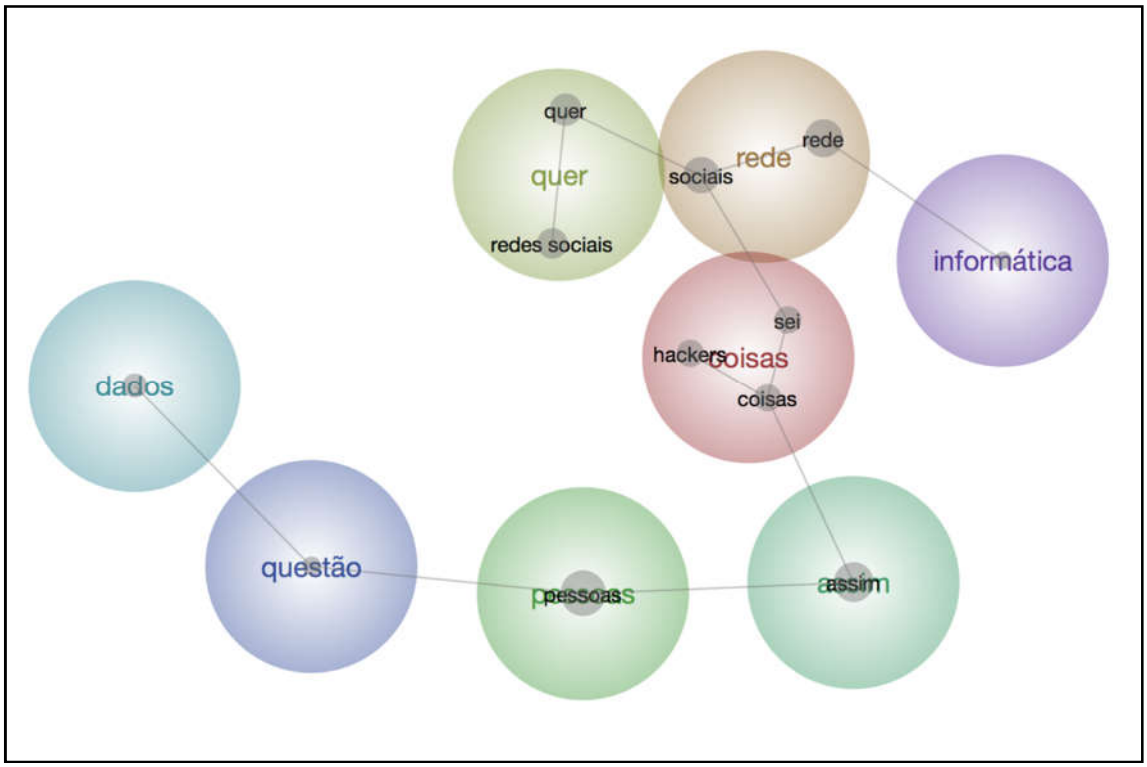

Figura 23 - Entrevistas – Segurança

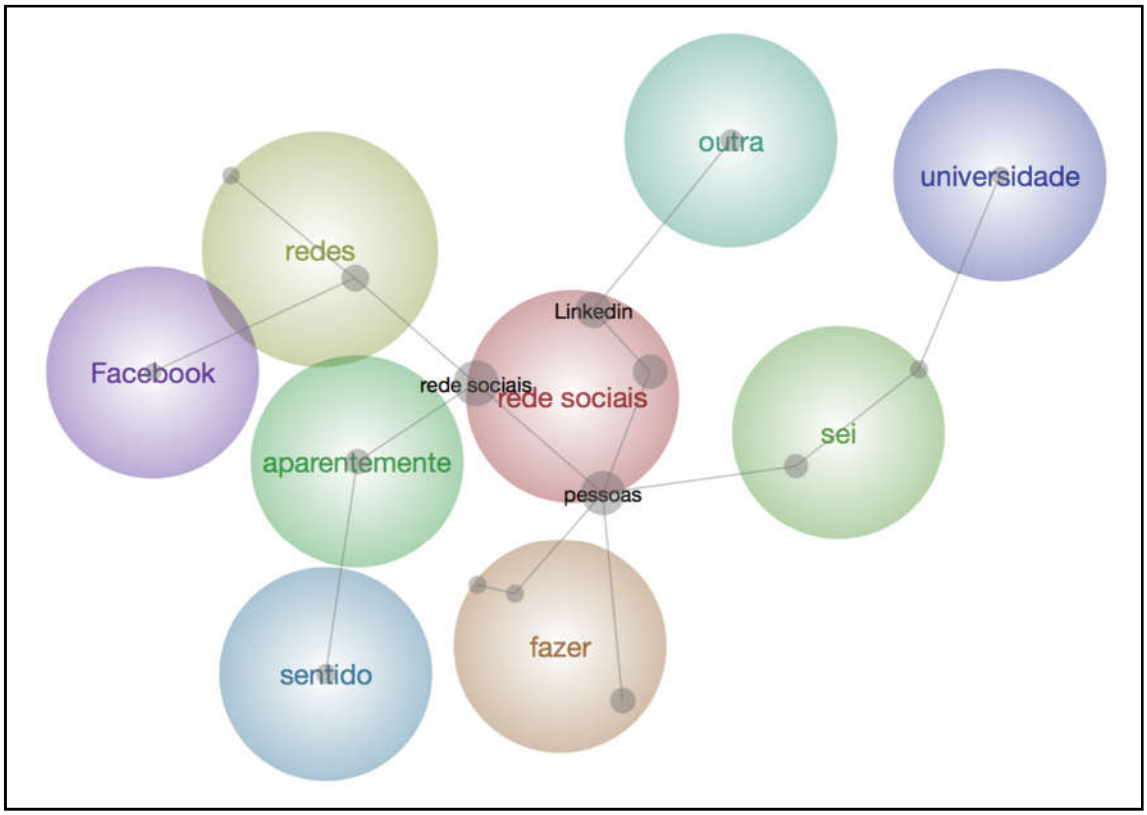

Figura 24 - Entrevistas – Confiança

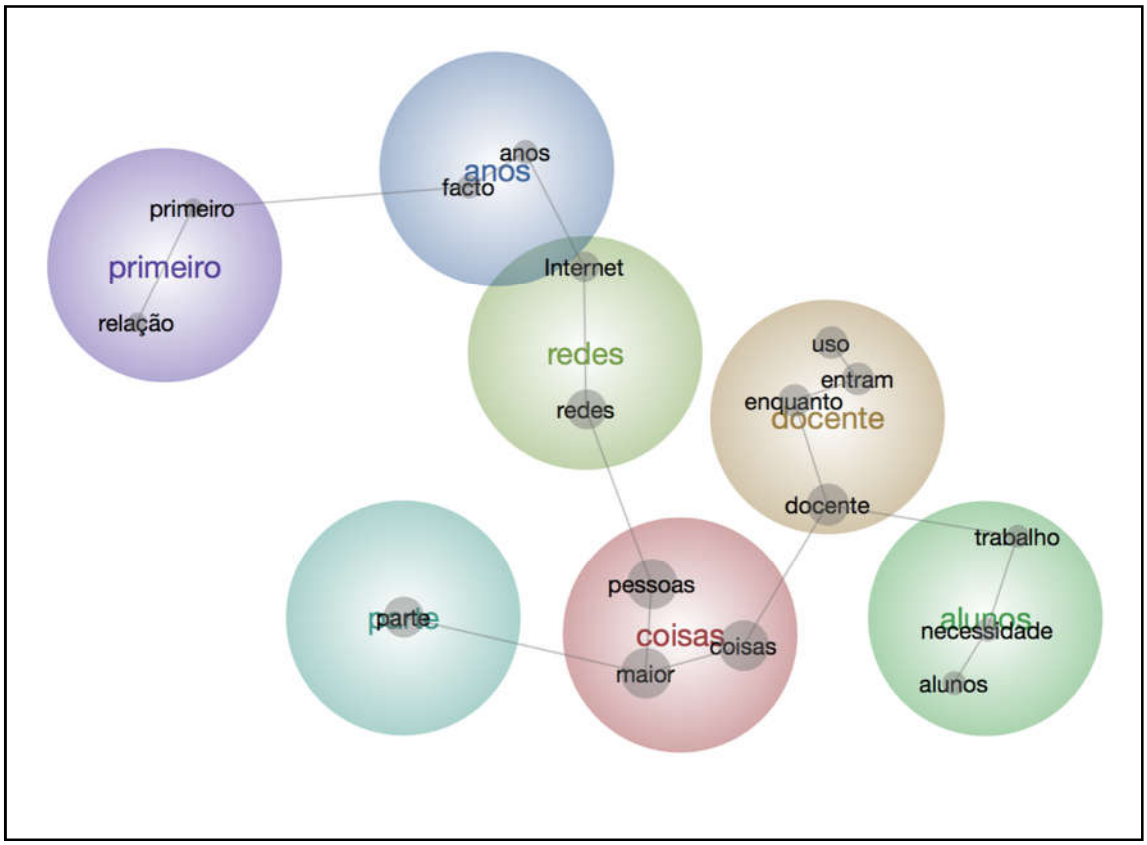

Figura 25 - Entrevistas – Consciência

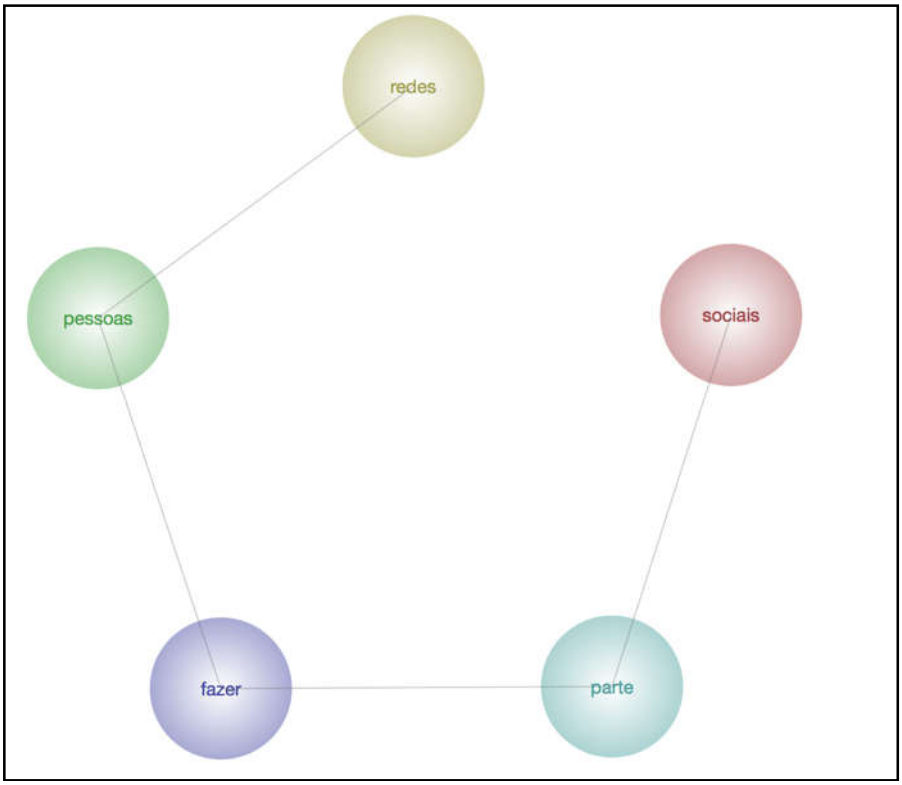

Figura 26 - Entrevistas – Recolha

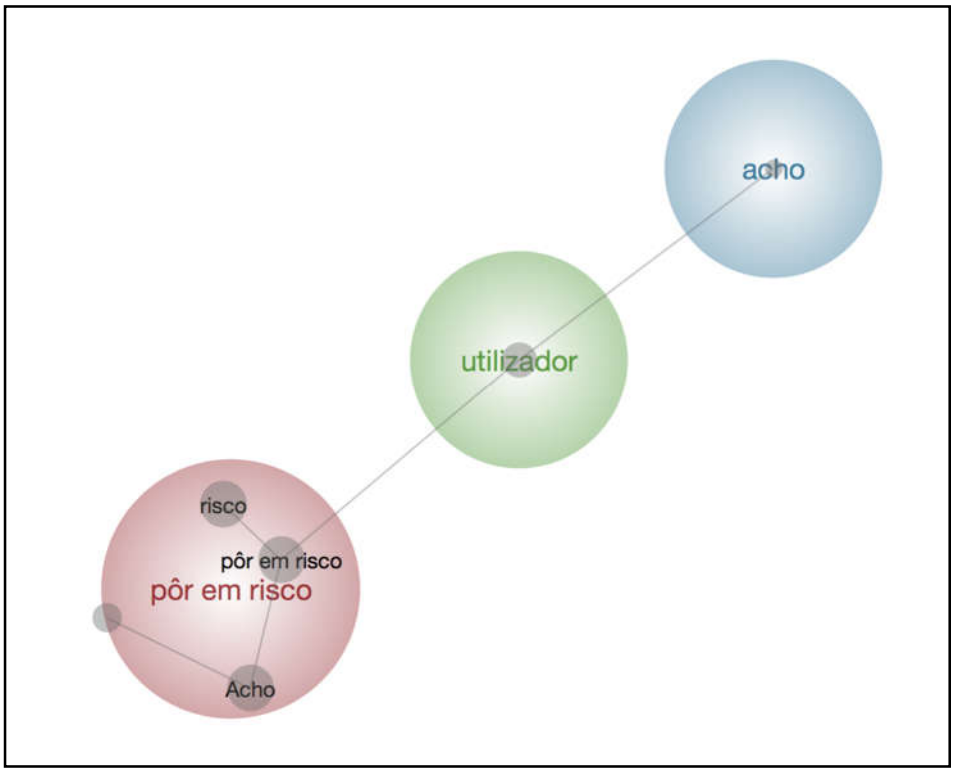

Figura 27 - Entrevistas - Uso secundário

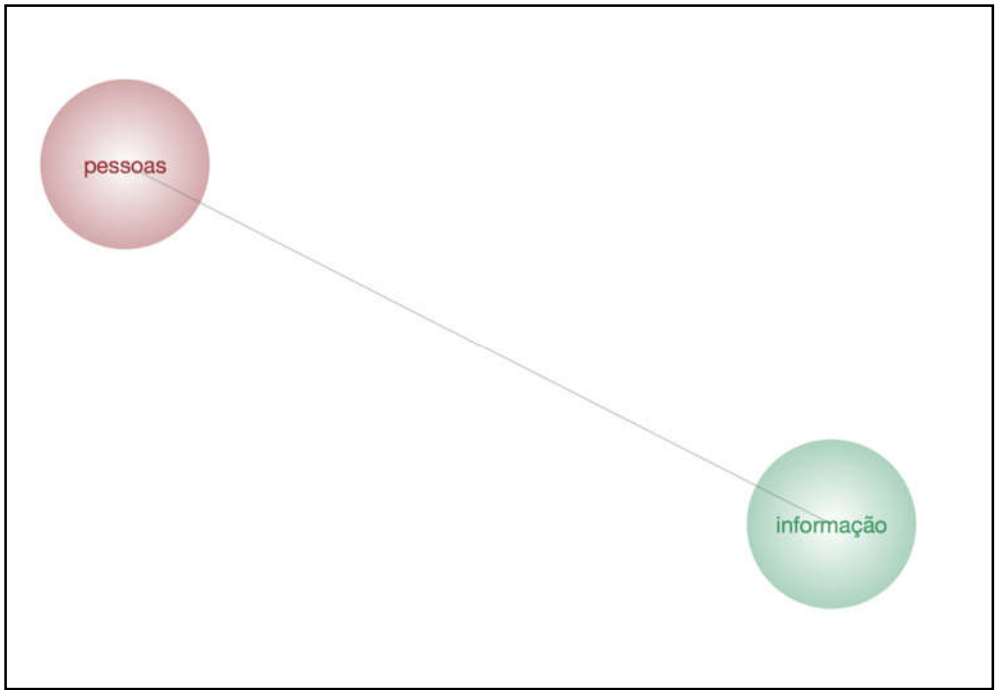

Figura 28 - Entrevistas - Riscos

Apêndice D – Questionário

Introdução do Questionário

Este questionário destina-se a recolher dados para uma dissertação de mestrado cujo principal objetivo é compreender como é que os estudantes universitários percecionam as redes sociais, como as utilizam e o que expõem online.

Todos os dados recolhidos serão tratados de forma totalmente anónima e estritamente confidencial, sendo exclusivamente usados para fins científicos.

Esperamos que possa responder da forma mais sincera e espontânea possível. Não existem respostas certas ou erradas. Poderá abandonar o questionário a qualquer momento, se assim o desejar.

O tempo necessário para preencher este questionário é de alguns minutos.

Agradecemos, desde já, pela sua disponibilidade em colaborar connosco.

Muito obrigado!

Nelson Rodrigues (Mestrado em Gestão de Sistemas de Informação | ISCTE-IUL)

Nota: Se houver alguma questão que nos queira colocar, ou se pretender algum feedback deste projeto, poderá contactar-nos através do email: nelson_jorge_rodrigues@iscte-iul.pt

Questões

Parte I

Idade: ____ anos

Sexo: ○ Feminino | ○ Masculino

Morada atual (enquanto estudante): [Concelhos] ⬇

Morada de origem: [Concelhos] ⬇

Universidade / Instituição de Ensino Superior a frequentar: [Instituições de Ensino] ⬇

Tipo de curso a frequentar: ○ Licenciatura | ○ Mestrado | ○ Doutoramento | ○ Outro

Curso a frequentar:

_____

Ano escolar a frequentar: ○ 1 | ○ 2 | ○ 3 | ○ 4 | ○ 5

Parte II

1. Indique por favor com que frequência usa cada uma das seguintes redes sociais online:

	Nunca	Raramente	Por vezes	Frequentemente	Muito frequentemente
Academia.edu					
Baidu Tieba					
Facebook					
Facebook Messenger					
Flickr					
Google+					
Hi5					
Instagram					
LINE					
LinkedIn					
MySpace					
Pinterest					
QQ					
Reddit					
Sina Weibo					
Skype					
Snapchat					
Telegram					
Tumblr					
Twitter					
Viber					
WeChat					
WhatsApp					
YouTube					
Outra 1					
Outra 2					

2. Em termos de <u>privacidade</u> nas redes sociais, até que ponto considera importante... (Escala: 1:Nada importante, 2: Pouco importante, 3: Moderadamente importante, 4: Importante, 5: Muito importante):

	1	2	3	4	5
A publicidade existente na rede social estar otimizada para o meu perfil de consumidor (e só serem mostrados anúncios relevantes para mim).					

A rede social ter uma política de privacidade clara, simples e de fácil compreensão					
Dispor de processos eficazes para resolver situações de violação de privacidade					
Não divulgar a minha localização, quer por intermédio de mensagens, quer por fotografias ou vídeos.					
Não fornecer informação privada/pessoal nas redes sociais					
Poder contar com a rede social para proteger a minha privacidade					
Poder controlar e gerir o nível de privacidade da minha informação/perfil na rede social					
Poder gerir que (outras) entidades/organizações podem aceder a informações sobre mim					
Remover a permissão de acesso à informação de localização às "Apps" de redes sociais.					
Saber como é que as minhas informações pessoais serão usadas					
Saber se a informação da rede social é vendida ou cedida a outras organizações					

3. Em termos de segurança nas redes sociais, até que ponto considera importante... (Escala: 1:Nada importante, 2: Pouco importante, 3: Moderadamente importante, 4: Importante, 5: Muito importante):

	1	2	3	4	5
A rede social deve oferecer mecanismos de autenticação reforçados (por exemplo: autenticação a 2 fatores (password + código), autenticação com certificados pessoais, obrigatoriedade de usar passwords muito complexas, etc.)					
A rede social garantir um elevado nível de segurança					
A rede social possibilitar um elevado nível de privacidade					
A rede social ter (por defeito) as funcionalidades que usam a localização desligadas ou desativadas.					
Ao usar uma rede social ter o cuidado de não revelar informação pessoal ou confidencial					
Conhecer a honestidade das redes sociais relativamente ao uso que fazem da informação dada pelos utilizadores					
Dispor de mecanismos ativos para mitigar o roubo de identidade					
Não partilhar informações que poderão vir a ser usadas de formas que não prevejo					
Poder autorizar explicitamente que organizações podem aceder aos meus dados					
Poder definir para cada entidade/organização, quais os dados/informações a que permito o acesso					
Saber que a minha informação só pode ser acedida por mim (por exemplo, usando mecanismos de encriptação)					

Saber que toda a informação fornecida à rede social está segura (de outros utilizadores ou agentes exteriores)					
Ter a garantia de que a informação fornecida à rede social não pode ser alterada por terceiros					
Ter a garantia de que pessoas não autorizadas não tenham acesso às minhas informações pessoais					

4. Qual o tipo de utilização que faz das redes sociais online (Escala: 1:Nunca, 2: Quase nunca, 3: Às vezes, 4: Frequentemente, 5: Muito frequentemente):

	1	2	3	4	5
Aceitar e fazer pedidos de amizade					
Avaliar, classificar e dar recomendações a produtos, serviços ou empresas					
Comentar "posts" e mensagens de outras pessoas					
Conversas através de mensagens instantâneas (Chat)					
Criar e agendar eventos					
Criar e dinamizar grupos de interesse ou comunidades					
Criar e manter diários detalhados de viagens ou experiências					
Dar donativos e apoiar causas					
Fazer Gostos/Likes/Love, etc. ...					
Fazer inquéritos e sondagens					
Fazer parte de grupos de interesse ou comunidades					
Identificar amigos					
Jogar jogos on-line					
Manter contacto com amigos e familiares distantes					
Manter contacto com antigos amigos					
Ouvir música e vídeos					
Participar em concursos, sorteios e inquéritos					
Partilhar a minha localização					
Partilhar álbuns fotográficos e vídeos					
Partilhar conteúdos cómicos					
Partilhar links, notícias e blogs					
Partilhar música e filmes					
Partilhar pensamentos e sentimentos					
Seguir informação sobre produtos, serviços e empresas					
Seguir personalidades públicas ou ídolos					
Sugerir amigos					
Usar aplicações oferecidas dentro da rede social					
Ver notícias e atualidades					

5. Pensando nas redes sociais que utiliza, qual a importância que atribui a cada uma das seguintes questões... (Escala: 1:Nada importante, 2: Pouco importante, 3: Moderadamente importante, 4: Importante, 5: Muito importante):

	1	2	3	4	5
Agiliza o contacto com colegas e professores					
Aproveitar ao máximo todos os momentos livres para verificar o estado nas redes sociais (na casa de banho, transportes públicos, filas de espera, etc...)					
As redes sociais online fazem parte da minha rotina diária					
Construir e manter uma rede de contactos profissionais					
Construir um perfil público com vista a maximizar a exposição e o *networking*					
Diversão ao passar tempo nas redes sociais					
Divulgar dados pessoais online ajuda-me a cultivar bons relacionamentos					
Divulgar dados pessoais online satisfaz as minhas necessidades sociais (de alguma forma)					
Organizar grupos de trabalho para atividades de estudo					
Partilhar coisas sobre mim com contactos casuais					
Produzir conteúdos relevantes para a minha atividade profissional					
Partilhar o meu dia-a-dia					
Procurar formas de controlar o que as pessoas me podem enviar (por exemplo: caixas de seleção que permitem desativar determinadas funcionalidades)					
Relaxar e descomprimir nas redes sociais					
Reunir rapidamente e em tempo real informação ou notícias atualizada/s sobre a minha cidade, país ou mundo					
Sinto que faço parte da comunidade da rede social que mais uso					
Sinto-me sem contacto quando não estou ligado a uma rede social online por algum tempo					
Tenho orgulho em dizer às pessoas que estou nas redes sociais					
Ter um perfil muito detalhado nas redes sociais					
Usar as redes sociais como mostruário para divulgar uma atividade profissional ou hobby					

6. Pensando na sua exposição online nas redes sociais, qual o nível de concordância que atribui a cada uma das seguintes afirmações... (Escala: 1:Discordo totalmente, 2: Discordo parcialmente, 3: Não concordo, nem discordo, 4: Concordo parcialmente, 5: Concordo totalmente):

	1	2	3	4	5
Certos contactos só têm acesso limitado aos meus dados					
Do meu perfil on-line é muito fácil entender que tipo de pessoa eu sou					
Estou convencido que a política de privacidade das redes sociais online garante a proteção da minha identidade					
Há muita coisa sobre mim que prefiro não falar com outras pessoas					

Incomoda-me quando tenho de colocar informação pessoal numa rede social					
Não falo de assuntos pessoais a menos que alguém o faça primeiro					
O meu perfil conta muito sobre mim					
O meu perfil é bem detalhado (por exemplo, partilho todas as empresas, escolas e locais onde já passei)					
Removo a minha identificação de imagens/vídeos colocados pelos meus contactos					
Revelo muita informação sobre mim.					
Se eu tivesse um diário nunca o mostraria a ninguém					
Vejo-me obrigado a fornecer informações pessoais contra a minha vontade					

7. O que pensa da privacidade pessoal ao usar as Redes Sociais?

8. Que tipos de problemas associa ao uso da internet e, em particular, das redes sociais?

Apêndice E – Estatísticas descritivas (Frequência, médias e desvio-padrão)

Parte I - Universidade | Instituição de ensino superior a Frequentar

Tabela de frequências de alunos por instituição de ensino superior

	N	%
Atlântica - Escola Universitária de Ciências Empresariais	1	0,4%
Escola Superior de Artes e Design	2	0,8%
Escola Superior de Educação de Paula Frassinetti	1	0,4%
Instituto Politécnico da Guarda	1	0,4%
Instituto Politécnico de Castelo Branco	2	0,8%
Instituto Politécnico de Leiria	4	1,6%
Instituto Politécnico de Lisboa	2	0,8%
Instituto Politécnico de Setúbal	1	0,4%
Instituto Politécnico de Tomar	1	0,4%
Instituto Politécnico do Porto	1	0,4%
Instituto Português de Administração de Marketing de Lisboa	1	0,4%
Instituto Superior de Ciências da Saúde Egas Moniz	1	0,4%
ISCTE - Instituto Universitário de Lisboa	55	21,3%
ISEC Lisboa - Instituto Superior de Educação e Ciências	1	0,4%
Universidade Autónoma de Lisboa Luís de Camões	2	0,8%
Universidade Católica Portuguesa	5	1,9%
Universidade da Beira Interior	4	1,6%
Universidade de Aveiro	60	23,3%
Universidade de Coimbra	2	0,8%
Universidade de Évora	3	1,2%
Universidade de Lisboa	58	22,5%
Universidade do Minho	1	0,4%
Universidade do Porto	2	0,8%
Universidade Europeia	1	0,4%
Universidade Lusíada	5	1,9%
Universidade Lusíada - Norte	1	0,4%
Universidade Nova de Lisboa	38	14,7%
Outra...	2	0,8%
Total	258	100%

Parte II – 1. Com que frequência utiliza as seguintes redes sociais online?

Tabela de frequências de uso das redes sociais

	Nunca		Raramente		Por vezes		Frequentemente		Muito frequentemente	
	N	%	N	%	N	%	N	%	N	%
Academia.edu	213	84,2%	21	8,3%	11	4,3%	7	2,8%	1	0,4%
Baidu Tieba	249	98,4%	2	0,8%	1	0,4%	0	0,0%	1	0,4%
Facebook	9	3,6%	8	3,2%	35	13,8%	86	34,0%	115	45,5%
Facebook Messenger	8	3,2%	4	1,6%	20	7,9%	58	22,9%	163	64,4%
Flickr	227	89,7%	22	8,7%	4	1,6%	0	0,0%	0	0,0%
Google+	123	48,6%	58	22,9%	41	16,2%	16	6,3%	15	5,9%
Hi5	238	94,1%	13	5,1%	2	0,8%	0	0,0%	0	0,0%
Instagram	43	17,0%	8	3,2%	15	5,9%	47	18,6%	140	55,3%
LINE	248	98,0%	3	1,2%	1	0,4%	1	0,4%	0	0,0%
LinkedIn	117	46,2%	44	17,4%	43	17,0%	32	12,6%	17	6,7%
MySpace	247	97,6%	5	2,0%	1	0,4%	0	0,0%	0	0,0%
Pinterest	129	51,0%	51	20,2%	46	18,2%	17	6,7%	10	4,0%
QQ	251	99,2%	1	0,4%	1	0,4%	0	0,0%	0	0,0%
Reddit	202	79,8%	20	7,9%	12	4,7%	12	4,7%	7	2,8%
Sina Weibo	251	99,2%	1	0,4%	1	0,4%	0	0,0%	0	0,0%
Skype	61	24,1%	89	35,2%	59	23,3%	32	12,6%	12	4,7%
Snapchat	148	58,5%	68	26,9%	29	11,5%	6	2,4%	2	0,8%
Telegram	244	96,4%	4	1,6%	1	0,4%	2	0,8%	2	0,8%
Tumblr	190	75,1%	34	13,4%	15	5,9%	8	3,2%	6	2,4%
Twitter	152	60,1%	40	15,8%	26	10,3%	17	6,7%	18	7,1%
Viber	224	88,5%	13	5,1%	9	3,6%	4	1,6%	3	1,2%
WeChat	248	98,0%	2	0,8%	1	0,4%	2	0,8%	0	0,0%
WhatsApp	42	16,6%	20	7,9%	45	17,8%	47	18,6%	99	39,1%
YouTube	3	1,2%	5	2,0%	32	12,6%	75	29,6%	138	54,5%

Tabela de média e desvio padrão de uso de redes sociais

	N	Média	Desvio-padrão
Academia.edu	253	1,27	,71
Baidu Tieba	253	1,03	,29
Facebook	253	4,15	1,01
Facebook Messenger	253	4,44	,94
Flickr	253	1,12	,37
Google+	253	1,98	1,20
Hi5	253	1,07	,28
Instagram	253	3,92	1,51
LINE	253	1,03	,25
LinkedIn	253	2,16	1,31
MySpace	253	1,03	,19
Pinterest	253	1,92	1,15
QQ	253	1,01	,14
Reddit	253	1,43	,98
Sina Weibo	253	1,01	,14
Skype	253	2,39	1,12
Snapchat	253	1,60	,84
Telegram	253	1,08	,47
Tumblr	253	1,44	,92
Twitter	253	1,85	1,26
Viber	253	1,22	,69
WeChat	253	1,04	,31
WhatsApp	253	3,56	1,48
YouTube	253	4,34	,86

Parte II – 2. O que considera importante em termos de privacidade nas redes sociais?

Tabela de frequências de nível de importância em termos de privacidade nas redes sociais

	Nada importante		Pouco importante		Moderadamente importante	
	N	%	N	%	N	%
A publicidade existente na rede social estar otimizada para o meu perfil de consumidor (e só serem mostrados anúncios relevantes para mim)	23	9,9%	39	16,8%	68	29,3%
A rede social ter uma política de privacidade clara, simples e de fácil compreensão	1	0,4%	3	1,3%	11	4,7%
Dispor de processos eficazes para resolver situações de violação de privacidade	1	0,4%	1	0,4%	5	2,2%
Não divulgar a minha localização, quer por intermédio de mensagens, quer por fotografias ou vídeos	0	0,0%	5	2,2%	21	9,1%
Não fornecer informação privada/pessoal nas redes sociais	0	0,0%	2	0,9%	13	5,6%
Poder contar com a rede social para proteger a minha privacidade	5	2,2%	5	2,2%	17	7,3%
Poder controlar e gerir o nível de privacidade da minha informação/perfil na rede social	0	0,0%	1	0,4%	5	2,2%
Poder gerir que (outras) entidades/organizações podem aceder a informações sobre mim	0	0,0%	2	0,9%	8	3,4%
Remover a permissão de acesso à informação de localização às "Apps" de redes sociais	1	0,4%	3	1,3%	13	5,6%
Saber como é que as minhas informações pessoais serão usadas	0	0,0%	0	0,0%	9	3,9%
Saber se a informação da rede social é vendida ou cedida a outras organizações	1	0,4%	1	0,4%	10	4,3%

	Importante		Muito importante	
	N	%	N	%
A publicidade existente na rede social estar otimizada para o meu perfil de consumidor (e só serem mostrados anúncios relevantes para mim)	64	27,6%	38	16,4%
A rede social ter uma política de privacidade clara, simples e de fácil compreensão	53	22,8%	164	70,7%
Dispor de processos eficazes para resolver situações de violação de privacidade	48	20,7%	177	76,3%
Não divulgar a minha localização, quer por intermédio de mensagens, quer por fotografias ou vídeos	62	26,7%	144	62,1%
Não fornecer informação privada/pessoal nas redes sociais	46	19,8%	171	73,7%
Poder contar com a rede social para proteger a minha privacidade	45	19,4%	160	69,0%

	Importante		Muito importante	
	N	%	N	%
Poder controlar e gerir o nível de privacidade da minha informação/perfil na rede social	40	17,2%	186	80,2%
Poder gerir que (outras) entidades/organizações podem aceder a informações sobre mim	43	18,5%	179	77,2%
Remover a permissão de acesso à informação de localização às "Apps" de redes sociais	64	27,6%	151	65,1%
Saber como é que as minhas informações pessoais serão usadas	47	20,3%	176	75,9%
Saber se a informação da rede social é vendida ou cedida a outras organizações	49	21,1%	171	73,7%

Tabela de média e desvio padrão de nível de importância em termos de privacidade nas redes sociais

	N	Média	Desvio-padrão
A publicidade existente na rede social estar otimizada para o meu perfil de consumidor (e só serem mostrados anúncios relevantes para mim)	232	3,24	1,20
A rede social ter uma política de privacidade clara, simples e de fácil compreensão	232	4,62	,68
Dispor de processos eficazes para resolver situações de violação de privacidade	232	4,72	,57
Não divulgar a minha localização, quer por intermédio de mensagens, quer por fotografias ou vídeos	232	4,49	,75
Não fornecer informação privada/pessoal nas redes sociais	232	4,66	,62
Poder contar com a rede social para proteger a minha privacidade	232	4,51	,89
Poder controlar e gerir o nível de privacidade da minha informação/perfil na rede social	232	4,77	,50
Poder gerir que (outras) entidades/organizações podem aceder a informações sobre mim	232	4,72	,57
Remover a permissão de acesso à informação de localização às "Apps" de redes sociais	232	4,56	,70
Saber como é que as minhas informações pessoais serão usadas	232	4,72	,53
Saber se a informação da rede social é vendida ou cedida a outras organizações	232	4,67	,62

Parte II – 3. O que considera importante em termos de segurança nas redes sociais?

Tabela de frequências de nível de importância em termos de segurança nas redes sociais

	Nada importante		Pouco importante		Moderadamente importante	
	N	%	N	%	N	%
A rede social deve oferecer mecanismos de autenticação reforçados (por exemplo: autenticação a 2 fatores (password + código), autenticação com certificados pessoais, obrigatoriedade de usar passwords muito complexas, etc.)	1	0,5%	11	5,0%	41	18,7%
A rede social garantir um elevado nível de segurança	0	0,0%	1	0,5%	5	2,3%
A rede social possibilitar um elevado nível de privacidade	0	0,0%	2	0,9%	6	2,7%
A rede social ter (por defeito) as funcionalidades que usam a localização desligadas ou desativadas	0	0,0%	5	2,3%	31	14,2%
Ao usar uma rede social ter o cuidado de não revelar informação pessoal ou confidencial	0	0,0%	1	0,5%	5	2,3%
Conhecer a honestidade das redes sociais relativamente ao uso que fazem da informação dada pelos utilizadores	0	0,0%	1	0,5%	10	4,6%
Dispor de mecanismos ativos para mitigar o roubo de identidade	0	0,0%	0	0,0%	8	3,7%
Não partilhar informações que poderão vir a ser usadas de formas que não prevejo	0	0,0%	1	0,5%	10	4,6%
Poder autorizar explicitamente que organizações podem aceder aos meus dados	2	0,9%	5	2,3%	11	5,0%
Poder definir para cada entidade/organização, quais os dados/informações a que permito o acesso	0	0,0%	2	0,9%	18	8,2%
Saber que a minha informação só pode ser acedida por mim (por exemplo, usando mecanismos de encriptação)	0	0,0%	1	0,5%	11	5,0%
Saber que toda a informação fornecida à rede social está segura (de outros utilizadores ou agentes exteriores)	0	0,0%	1	0,5%	7	3,2%
Ter a garantia de que a informação fornecida à rede social não pode ser alterada por terceiros	0	0,0%	0	0,0%	2	0,9%
Ter a garantia de que pessoas não autorizadas não tenham acesso às minhas informações pessoais	0	0,0%	2	0,9%	3	1,4%

	Importante		Muito importante	
	N	%	N	%
A rede social deve oferecer mecanismos de autenticação reforçados (por exemplo: autenticação a 2 fatores (password + código), autenticação com certificados pessoais, obrigatoriedade de usar passwords muito complexas, etc.)	74	33,8%	92	42,0%
A rede social garantir um elevado nível de segurança	61	27,9%	152	69,4%

	Importante		Muito importante	
	N	%	N	%
A rede social possibilitar um elevado nível de privacidade	49	22,4%	162	74,0%
A rede social ter (por defeito) as funcionalidades que usam a localização desligadas ou desativadas	64	29,2%	119	54,3%
Ao usar uma rede social ter o cuidado de não revelar informação pessoal ou confidencial	65	29,7%	148	67,6%
Conhecer a honestidade das redes sociais relativamente ao uso que fazem da informação dada pelos utilizadores	72	32,9%	136	62,1%
Dispor de mecanismos ativos para mitigar o roubo de identidade	51	23,3%	160	73,1%
Não partilhar informações que poderão vir a ser usadas de formas que não prevejo	49	22,4%	159	72,6%
Poder autorizar explicitamente que organizações podem aceder aos meus dados	70	32,0%	131	59,8%
Poder definir para cada entidade/organização, quais os dados/informações a que permito o acesso	55	25,1%	144	65,8%
Saber que a minha informação só pode ser acedida por mim (por exemplo, usando mecanismos de encriptação)	54	24,7%	153	69,9%
Saber que toda a informação fornecida à rede social está segura (de outros utilizadores ou agentes exteriores)	54	24,7%	157	71,7%
Ter a garantia de que a informação fornecida à rede social não pode ser alterada por terceiros	47	21,5%	170	77,6%
Ter a garantia de que pessoas não autorizadas não tenham acesso às minhas informações pessoais	33	15,1%	181	82,6%

Tabela de média e desvio padrão de nível de importância em termos de segurança nas redes sociais

	N	Média	Desvio-padrão
A rede social deve oferecer mecanismos de autenticação reforçados (por exemplo: autenticação a 2 fatores (password + código), autenticação com certificados pessoais, obrigatoriedade de usar passwords muito complexas, etc.)	219	4,12	,92
A rede social garantir um elevado nível de segurança	219	4,66	,55
A rede social possibilitar um elevado nível de privacidade	219	4,69	,57
A rede social ter (por defeito) as funcionalidades que usam a localização desligadas ou desativadas	219	4,36	,81
Ao usar uma rede social ter o cuidado de não revelar informação pessoal ou confidencial	219	4,64	,55
Conhecer a honestidade das redes sociais relativamente ao uso que fazem da informação dada pelos utilizadores	219	4,57	,60

	N	Média	Desvio-padrão
Dispor de mecanismos ativos para mitigar o roubo de identidade	219	4,69	,54
Não partilhar informações que poderão vir a ser usadas de formas que não prevejo	219	4,67	,58
Poder autorizar explicitamente que organizações podem aceder aos meus dados	219	4,47	,77
Poder definir para cada entidade/organização, quais os dados/informações a que permito o acesso	219	4,56	,68
Saber que a minha informação só pode ser acedida por mim (por exemplo, usando mecanismos de encriptação)	219	4,64	,60
Saber que toda a informação fornecida à rede social está segura (de outros utilizadores ou agentes exteriores)	219	4,68	,56
Ter a garantia de que a informação fornecida à rede social não pode ser alterada por terceiros	219	4,77	,44
Ter a garantia de que pessoas não autorizadas não tenham acesso às minhas informações pessoais	219	4,79	,50

Parte II – 4. Qual o tipo de utilização das redes sociais?

Tabela de frequências de tipo de utilização das redes sociais

	Nunca		Quase nunca		Às vezes		Frequentemente	
	N	%	N	%	N	%	N	%
Aceitar e fazer pedidos de amizade	1	0,5%	41	19,2%	110	51,6%	49	23,0%
Avaliar, classificar e dar recomendações a produtos, serviços ou empresas	53	24,9%	92	43,2%	55	25,8%	12	5,6%
Comentar "posts" e mensagens de outras pessoas	10	4,7%	50	23,5%	84	39,4%	56	26,3%
Conversas através de mensagens instantâneas (Chat)	5	2,3%	6	2,8%	21	9,9%	49	23,0%
Criar e agendar eventos	34	16,0%	71	33,3%	59	27,7%	39	18,3%
Criar e dinamizar grupos de interesse ou comunidades	51	23,9%	67	31,5%	57	26,8%	28	13,1%
Criar e manter diários detalhados de viagens ou experiências	112	52,6%	62	29,1%	28	13,1%	10	4,7%
Dar donativos e apoiar causas	130	61,0%	55	25,8%	23	10,8%	4	1,9%
Fazer Gostos/Likes/Love, etc. ...	6	2,8%	18	8,5%	56	26,3%	69	32,4%
Fazer inquéritos e sondagens	63	29,6%	67	31,5%	62	29,1%	19	8,9%
Fazer parte de grupos de interesse ou comunidades	19	8,9%	29	13,6%	68	31,9%	70	32,9%
Identificar amigos	27	12,7%	40	18,8%	69	32,4%	57	26,8%
Jogar jogos on-line	98	46,0%	59	27,7%	33	15,5%	14	6,6%

	Nunca		Quase nunca		Às vezes		Frequentemente	
	N	%	N	%	N	%	N	%
Manter contacto com amigos e familiares distantes	6	2,8%	26	12,2%	58	27,2%	72	33,8%
Manter contacto com antigos amigos	4	1,9%	30	14,1%	70	32,9%	69	32,4%
Ouvir música e vídeos	14	6,6%	21	9,9%	39	18,3%	59	27,7%
Participar em concursos, sorteios e inquéritos	78	36,6%	67	31,5%	46	21,6%	18	8,5%
Partilhar a minha localização	103	48,4%	71	33,3%	31	14,6%	8	3,8%
Partilhar álbuns fotográficos e vídeos	47	22,1%	66	31,0%	63	29,6%	28	13,1%
Partilhar conteúdos cómicos	50	23,5%	60	28,2%	60	28,2%	35	16,4%
Partilhar links, notícias e blogs	42	19,7%	54	25,4%	72	33,8%	37	17,4%
Partilhar música e filmes	73	34,3%	65	30,5%	39	18,3%	31	14,6%
Partilhar pensamentos e sentimentos	114	53,5%	57	26,8%	26	12,2%	11	5,2%
Seguir informação sobre produtos, serviços e empresas	36	16,9%	45	21,1%	73	34,3%	46	21,6%
Seguir personalidades públicas ou ídolos	39	18,3%	39	18,3%	71	33,3%	48	22,5%
Sugerir amigos	114	53,5%	53	24,9%	30	14,1%	10	4,7%
Usar aplicações oferecidas dentro da rede social	74	34,7%	79	37,1%	44	20,7%	13	6,1%
Ver notícias e atualidades	7	3,3%	15	7,0%	50	23,5%	90	42,3%

	Muito frequentemente	
	N	%
Aceitar e fazer pedidos de amizade	12	5,6%
Avaliar, classificar e dar recomendações a produtos, serviços ou empresas	1	0,5%
Comentar “posts” e mensagens de outras pessoas	13	6,1%
Conversas através de mensagens instantâneas (Chat)	132	62,0%
Criar e agendar eventos	10	4,7%
Criar e dinamizar grupos de interesse ou comunidades	10	4,7%
Criar e manter diários detalhados de viagens ou experiências	1	0,5%
Dar donativos e apoiar causas	1	0,5%
Fazer Gostos/Likes/Love, etc. ...	64	30,0%
Fazer inquéritos e sondagens	2	0,9%
Fazer parte de grupos de interesse ou comunidades	27	12,7%
Identificar amigos	20	9,4%

	Muito frequentemente	
	N	%
Jogar jogos on-line	9	4,2%
Manter contacto com amigos e familiares distantes	51	23,9%
Manter contacto com antigos amigos	40	18,8%
Ouvir música e vídeos	80	37,6%
Participar em concursos, sorteios e inquéritos	4	1,9%
Partilhar a minha localização	0	0,0%
Partilhar álbuns fotográficos e vídeos	9	4,2%
Partilhar conteúdos cómicos	8	3,8%
Partilhar links, notícias e blogs	8	3,8%
Partilhar música e filmes	5	2,3%
Partilhar pensamentos e sentimentos	5	2,3%
Seguir informação sobre produtos, serviços e empresas	13	6,1%
Seguir personalidades públicas ou ídolos	16	7,5%
Sugerir amigos	6	2,8%
Usar aplicações oferecidas dentro da rede social	3	1,4%
Ver notícias e atualidades	51	23,9%

Tabela de média e desvio padrão de tipo de utilização das redes sociais

	N	Média	Desvio-padrão
Aceitar e fazer pedidos de amizade	213	3,14	,81
Avaliar, classificar e dar recomendações a produtos, serviços ou empresas	213	2,14	,87
Comentar "posts" e mensagens de outras pessoas	213	3,06	,96
Conversas através de mensagens instantâneas (Chat)	213	4,39	,94
Criar e agendar eventos	213	2,62	1,10
Criar e dinamizar grupos de interesse ou comunidades	213	2,43	1,13
Criar e manter diários detalhados de viagens ou experiências	213	1,71	,90
Dar donativos e apoiar causas	213	1,55	,80
Fazer Gostos/Likes/Love, etc. ...	213	3,78	1,06
Fazer inquéritos e sondagens	213	2,20	1,00
Fazer parte de grupos de interesse ou comunidades	213	3,27	1,12
Identificar amigos	213	3,01	1,16

	N	Média	Desvio-padrão
Jogar jogos on-line	213	1,95	1,12
Manter contacto com amigos e familiares distantes	213	3,64	1,06
Manter contacto com antigos amigos	213	3,52	1,01
Ouvir música e vídeos	213	3,80	1,23
Participar em concursos, sorteios e inquéritos	213	2,08	1,04
Partilhar a minha localização	213	1,74	,84
Partilhar álbuns fotográficos e vídeos	213	2,46	1,10
Partilhar conteúdos cómicos	213	2,49	1,13
Partilhar links, notícias e blogs	213	2,60	1,10
Partilhar música e filmes	213	2,20	1,13
Partilhar pensamentos e sentimentos	213	1,76	1,01
Seguir informação sobre produtos, serviços e empresas	213	2,79	1,14
Seguir personalidades públicas ou ídolos	213	2,83	1,19
Sugerir amigos	213	1,78	1,04
Usar aplicações oferecidas dentro da rede social	213	2,02	,96
Ver notícias e atualidades	213	3,77	1,00

Parte II – 5. O que considera importante em termos da utilização das redes sociais?

Tabela de frequências de importância na utilização das redes sociais

	Nada importante		Pouco importante		Moderadamente importante	
	N	%	N	%	N	%
Agiliza o contacto com colegas e professores	10	5,0%	12	6,0%	43	21,5%
Aproveitar ao máximo todos os momentos livres para verificar o estado nas redes sociais (na casa de banho, transportes públicos, filas de espera, etc...)	29	14,5%	77	38,5%	55	27,5%
As redes sociais online fazem parte da minha rotina diária	13	6,5%	36	18,0%	75	37,5%
Construir e manter uma rede de contactos profissionais	7	3,5%	27	13,5%	78	39,0%
Construir um perfil público com vista a maximizar a exposição e o *networking*	33	16,5%	45	22,5%	61	30,5%
Diversão ao passar tempo nas redes sociais	13	6,5%	42	21,0%	69	34,5%
Divulgar dados pessoais online ajuda-me a cultivar bons relacionamentos	102	51,0%	64	32,0%	23	11,5%

	Nada importante		Pouco importante		Moderadamente importante	
	N	%	N	%	N	%
Divulgar dados pessoais online satisfaz as minhas necessidades sociais (de alguma forma)	116	58,0%	46	23,0%	30	15,0%
Organizar grupos de trabalho para atividades de estudo	17	8,5%	29	14,5%	53	26,5%
Partilhar coisas sobre mim com contactos casuais	90	45,0%	71	35,5%	29	14,5%
Partilhar conteúdos relevantes para a minha atividade profissional	34	17,0%	40	20,0%	71	35,5%
Partilhar o meu dia-a-dia	107	53,5%	64	32,0%	19	9,5%
Procurar formas de controlar o que as pessoas me podem enviar (por exemplo: caixas de seleção que permitem desativar determinadas funcionalidades)	29	14,5%	36	18,0%	54	27,0%
Relaxar e descomprimir nas redes sociais	10	5,0%	47	23,5%	68	34,0%
Reunir rapidamente e em tempo real informação ou notícias atualizada/s sobre a minha cidade, país ou mundo	8	4,0%	23	11,5%	49	24,5%
Sinto que faço parte da comunidade da rede social que mais uso	46	23,0%	67	33,5%	54	27,0%
Sinto-me sem contacto quando não estou ligado a uma rede social online por algum tempo	72	36,0%	55	27,5%	45	22,5%
Tenho orgulho em dizer às pessoas que estou nas redes sociais	109	54,5%	66	33,0%	18	9,0%
Ter um perfil muito detalhado nas redes sociais	114	57,0%	57	28,5%	22	11,0%
Usar as redes sociais como mostruário para divulgar uma atividade profissional ou hobby	60	30,0%	49	24,5%	62	31,0%

	Importante		Muito importante	
	N	%	N	%
Agiliza o contacto com colegas e professores	79	39,5%	56	28,0%
Aproveitar ao máximo todos os momentos livres para verificar o estado nas redes sociais (na casa de banho, transportes públicos, filas de espera, etc...)	25	12,5%	14	7,0%
As redes sociais online fazem parte da minha rotina diária	50	25,0%	26	13,0%
Construir e manter uma rede de contactos profissionais	59	29,5%	29	14,5%
Construir um perfil público com vista a maximizar a exposição e o *networking*	44	22,0%	17	8,5%
Diversão ao passar tempo nas redes sociais	51	25,5%	25	12,5%
Divulgar dados pessoais online ajuda-me a cultivar bons relacionamentos	7	3,5%	4	2,0%
Divulgar dados pessoais online satisfaz as minhas necessidades sociais (de alguma forma)	6	3,0%	2	1,0%

	Importante		Muito importante	
	N	%	N	%
Organizar grupos de trabalho para atividades de estudo	68	34,0%	33	16,5%
Partilhar coisas sobre mim com contactos casuais	6	3,0%	4	2,0%
Partilhar conteúdos relevantes para a minha atividade profissional	38	19,0%	17	8,5%
Partilhar o meu dia-a-dia	5	2,5%	5	2,5%
Procurar formas de controlar o que as pessoas me podem enviar (por exemplo: caixas de seleção que permitem desativar determinadas funcionalidades)	50	25,0%	31	15,5%
Relaxar e descomprimir nas redes sociais	50	25,0%	25	12,5%
Reunir rapidamente e em tempo real informação ou notícias atualizada/s sobre a minha cidade, país ou mundo	74	37,0%	46	23,0%
Sinto que faço parte da comunidade da rede social que mais uso	22	11,0%	11	5,5%
Sinto-me sem contacto quando não estou ligado a uma rede social online por algum tempo	21	10,5%	7	3,5%
Tenho orgulho em dizer às pessoas que estou nas redes sociais	4	2,0%	3	1,5%
Ter um perfil muito detalhado nas redes sociais	3	1,5%	4	2,0%
Usar as redes sociais como mostruário para divulgar uma atividade profissional ou hobby	23	11,5%	6	3,0%

Tabela de média e desvio padrão de importância na utilização das redes sociais

	N	Média	Desvio-padrão
Agiliza o contacto com colegas e professores	200	3,80	1,07
Aproveitar ao máximo todos os momentos livres para verificar o estado nas redes sociais (na casa de banho, transportes públicos, filas de espera, etc...)	200	2,59	1,10
As redes sociais online fazem parte da minha rotina diária	200	3,20	1,08
Construir e manter uma rede de contactos profissionais	200	3,38	1,01
Construir um perfil público com vista a maximizar a exposição e o *networking*	200	2,84	1,19
Diversão ao passar tempo nas redes sociais	200	3,17	1,10
Divulgar dados pessoais online ajuda-me a cultivar bons relacionamentos	200	1,74	,94
Divulgar dados pessoais online satisfaz as minhas necessidades sociais (de alguma forma)	200	1,66	,91
Organizar grupos de trabalho para atividades de estudo	200	3,36	1,17
Partilhar coisas sobre mim com contactos casuais	200	1,82	,93
Partilhar conteúdos relevantes para a minha atividade profissional	200	2,82	1,18
Partilhar o meu dia-a-dia	200	1,69	,93

Procurar formas de controlar o que as pessoas me podem enviar (por exemplo: caixas de seleção que permitem desativar determinadas funcionalidades)	200	3,09	1,28
Relaxar e descomprimir nas redes sociais	200	3,17	1,08
Reunir rapidamente e em tempo real informação ou notícias atualizada/s sobre a minha cidade, país ou mundo	200	3,64	1,08
Sinto que faço parte da comunidade da rede social que mais uso	200	2,43	1,12
Sinto-me sem contacto quando não estou ligado a uma rede social online por algum tempo	200	2,18	1,14
Tenho orgulho em dizer às pessoas que estou nas redes sociais	200	1,63	,85
Ter um perfil muito detalhado nas redes sociais	200	1,63	,89
Usar as redes sociais como mostruário para divulgar uma atividade profissional ou hobby	200	2,33	1,11

Parte II – 6. Relativamente à exposição online nas redes sociais, concorda com as seguintes afirmações?

Tabela de frequências de concordância relativamente à exposição online nas redes sociais

	Discordo totalmente		**Discordo parcialmente**		**Não concordo, nem discordo**	
	N	%	N	%	N	%
Certos contactos só têm acesso limitado aos meus dados	2	1,1%	10	5,4%	24	13,0%
Do meu perfil on-line é muito fácil entender que tipo de pessoa eu sou	44	23,9%	42	22,8%	53	28,8%
Estou convencido que a política de privacidade das redes sociais online garante a proteção da minha identidade	13	7,1%	54	29,3%	49	26,6%
Há muita coisa sobre mim que prefiro não falar com outras pessoas	5	2,7%	2	1,1%	20	10,9%
Incomoda-me quando tenho de colocar informação pessoal numa rede social	3	1,6%	18	9,8%	43	23,4%
Não falo de assuntos pessoais a menos que alguém o faça primeiro	22	12,0%	30	16,3%	59	32,1%
Não me importo de colocar informações pessoais online	74	40,2%	53	28,8%	34	18,5%
O meu perfil conta muito sobre mim	66	35,9%	64	34,8%	38	20,7%
O meu perfil é bem detalhado (por exemplo, partilho todas as empresas, escolas e locais onde já passei)	66	35,9%	60	32,6%	31	16,8%
Removo a minha identificação de imagens/vídeos colocados pelos meus contactos	39	21,2%	53	28,8%	51	27,7%
Revelo muita informação sobre mim	85	46,2%	55	29,9%	28	15,2%
Se eu tivesse um diário nunca o mostraria a ninguém	7	3,8%	10	5,4%	25	13,6%
Vejo-me obrigado a fornecer informações pessoais contra a minha vontade	70	38,0%	40	21,7%	40	21,7%

	Concordo parcialmente		Concordo totalmente	
	N	%	N	%
Certos contactos só têm acesso limitado aos meus dados	53	28,8%	95	51,6%
Do meu perfil on-line é muito fácil entender que tipo de pessoa eu sou	39	21,2%	6	3,3%
Estou convencido que a política de privacidade das redes sociais online garante a proteção da minha identidade	56	30,4%	12	6,5%
Há muita coisa sobre mim que prefiro não falar com outras pessoas	54	29,3%	103	56,0%
Incomoda-me quando tenho de colocar informação pessoal numa rede social	54	29,3%	66	35,9%
Não falo de assuntos pessoais a menos que alguém o faça primeiro	49	26,6%	24	13,0%
Não me importo de colocar informações pessoais online	18	9,8%	5	2,7%
O meu perfil conta muito sobre mim	12	6,5%	4	2,2%
O meu perfil é bem detalhado (por exemplo, partilho todas as empresas, escolas e locais onde já passei)	20	10,9%	7	3,8%
Removo a minha identificação de imagens/vídeos colocados pelos meus contactos	27	14,7%	14	7,6%
Revelo muita informação sobre mim	9	4,9%	7	3,8%
Se eu tivesse um diário nunca o mostraria a ninguém	48	26,1%	94	51,1%
Vejo-me obrigado a fornecer informações pessoais contra a minha vontade	25	13,6%	9	4,9%

Tabela de média e desvio padrão de concordância relativamente à exposição online nas redes sociais

	N	Média	Desvio-padrão
Certos contactos só têm acesso limitado aos meus dados	184	4,24	,95
Do meu perfil on-line é muito fácil entender que tipo de pessoa eu sou	184	2,57	1,16
Estou convencido que a política de privacidade das redes sociais online garante a proteção da minha identidade	184	3,00	1,07
Há muita coisa sobre mim que prefiro não falar com outras pessoas	184	4,35	,92
Incomoda-me quando tenho de colocar informação pessoal numa rede social	184	3,88	1,06
Não falo de assuntos pessoais a menos que alguém o faça primeiro	184	3,13	1,19
Não me importo de colocar informações pessoais online	184	2,06	1,11
O meu perfil conta muito sobre mim	184	2,04	1,01

O meu perfil é bem detalhado (por exemplo, partilho todas as empresas, escolas e locais onde já passei)	184	2,14	1,14
Removo a minha identificação de imagens/vídeos colocados pelos meus contactos	184	2,59	1,19
Revelo muita informação sobre mim	184	1,90	1,07
Se eu tivesse um diário nunca o mostraria a ninguém	184	4,15	1,09
Vejo-me obrigado a fornecer informações pessoais contra a minha vontade	184	2,26	1,23

Apêndice F – Análise de Componentes Principais

Objetivo 1 - Análise de Componentes Principais – Questão 2 (Parte II)

KMO e Teste de Bartlett		
KMO		,772
Teste de Bartlett	Chi-Quadrado aprox.	524,065
	Graus de liberdade	28
	Sig.	,000

Variância total explicada

Componentes	Valores Próprios	% Variância Explicada	% Cumulativa	Valores Próprios	% Variância Explicada	% Cumulativa
1	3,318	41,479	41,479	3,318	41,479	41,479
2	1,205	15,057	56,536	1,205	15,057	56,536
3	,914	11,430	67,966			
4	,764	9,555	77,520			
5	,577	7,207	84,728			
6	,509	6,368	91,096			
7	,428	5,346	96,442			
8	,285	3,558	100,000			

Método de Extração: Análise de componentes principais

Matriz de Componentes

Componentes	1	2
1	,733	,681
2	-,681	,733

Método de Extração: Análise de componentes principais.
Método de rotação: Varimax e normalização de Kaiser.

Correlações

Componente 1 – Privacidade da rede social

	Dispor de processos eficazes para resolver situações de violação de privacidade	A rede social ter uma política de privacidade clara, simples e de fácil compreensão	Saber como é que as minhas informações pessoais serão usadas	Não divulgar a minha localização, quer por intermédio de mensagens, quer por fotografias ou vídeos
Dispor de processos eficazes para resolver situações de violação de privacidade	1			
	232			
A rede social ter uma política de privacidade clara, simples e de fácil compreensão	**,687*****	1		
	,000			
	232	232		
Saber como é que as minhas informações pessoais serão usadas	**,485*****	**,473*****	1	
	,000	,000		
	232	232	232	
Não divulgar a minha localização, quer por intermédio de mensagens, quer por fotografias ou vídeos	**,372*****	**,339*****	**,312*****	1
	,000	,000	,000	
	232	232	232	232
*** p < 0,001; ** p < 0,01; * p < 0,05				

Componente 2 – Capacidade de controlo da informação privada

	Remover a permissão de acesso à informação de localização às "Apps" de redes sociais	Não fornecer informação privada/pessoal nas redes sociais	Poder contar com a rede social para proteger a minha privacidade	Poder gerir que (outras) entidades/organizações podem aceder a informações sobre mim
Remover a permissão de acesso à informação de localização às "Apps" de redes sociais	1			
	232			
Não fornecer informação privada/pessoal nas redes sociais	**,371*****	1		
	,000			
	232	232		
Poder contar com a rede social para proteger a minha privacidade	**,253*****	**,420*****	1	
	,000	,000		
	232	232	232	
	,447***	**,295*****	**,369*****	1

	Remover a permissão de acesso à informação de localização às "Apps" de redes sociais	Não fornecer informação privada/pessoal nas redes sociais	Poder contar com a rede social para proteger a minha privacidade	Poder gerir que (outras) entidades/organizações podem aceder a informações sobre mim
Poder gerir que (outras) entidades/organizações podem aceder a informações sobre mim	,000	,000	,000	
	232	232	232	232
*** p < 0,001; ** p < 0,01; * p < 0,05				

Correlação entre as 2 dimensões obtidas

	Privacidade da rede social	Capacidade de controlo da informação privada
Privacidade da rede social	1	
	232	
Capacidade de controlo da informação privada	**,477*****	1
	,000	
	232	232
*** p < 0,001; ** p < 0,01; * p < 0,05		

Tabela de frequências de índices relativos às dimensões obtidas no objetivo 1

Privacidade da rede social		
	N	**%**
2,00	1	,4
3,00	3	1,3
3,25	2	,9
3,50	2	,9
3,75	10	4,3
4,00	17	7,3
4,25	17	7,3
4,50	29	12,5
4,75	48	20,7
5,00	103	44,4
Total	232	100,0

Capacidade de controlo da informação privada		
	N	**%**
2,75	1	,4
3,00	4	1,7
3,25	4	1,7
3,50	6	2,6
3,75	6	2,6
4,00	17	7,3
4,25	18	7,8
4,50	27	11,6
4,75	49	21,1
5,00	100	43,1
Total	232	100,0

Objetivo 2 - Análise de Componentes Principais – Questão 3 (Parte II)

KMO e Teste de Bartlett	
KMO	,886

Teste de Bartlett	Chi-Quadrado aprox.	1245,298
	Graus de liberdade	91
	Sig.	,000

Variância total explicada

Componentes	Valores Próprios	% Variância Explicada	% Cumulativa	Valores Próprios	% Variância Explicada	% Cumulativa
1	6,018	42,987	42,987	2,968	21,200	21,200
2	1,114	7,957	50,944	2,706	19,328	40,528
3	1,055	7,535	58,479	2,513	17,951	58,479
4	,896	6,400	64,879			
5	,759	5,419	70,298			
6	,749	5,348	75,646			
7	,611	4,362	80,009			
8	,542	3,868	83,877			
9	,488	3,485	87,362			
10	,449	3,207	90,569			
11	,394	2,815	93,384			
12	,359	2,567	95,950			
13	,340	2,427	98,377			
14	,227	1,623	100,000			

Método de Extração: Análise de componentes principais

Matriz de Componentes

Componentes	1	2	3
1	,617	,577	,536
2	,656	,000	-,755
3	-,435	,817	-,378

Método de Extração: Análise de componentes principais.
Método de rotação: Varimax e normalização de Kaiser.

Correlações

Componente 1 - Conhecimento de quem pode aceder à informação privada

	Poder autorizar explicitamente que organizações podem aceder aos meus dados	Poder definir para cada entidade/organização, quais os dados/informações a que permito o acesso	Não partilhar informações que poderão vir a ser usadas de formas que não prevejo	Conhecer a honestidade das redes sociais relativamente ao uso que fazem da informação dada pelos utilizadores	Dispor de mecanismos ativos para mitigar o roubo de identidade
Poder autorizar explicitamente que organizações podem aceder aos meus dados	1				
	219				
Poder definir para cada entidade/organização, quais os dados/informações a que permito o acesso	**,572*****	1			
	,000				
	219	219			
Não partilhar informações que poderão vir a ser usadas de formas que não prevejo	**,388*****	**,495*****	1		
	,000	,000			
	219	219	219		
Conhecer a honestidade das redes sociais relativamente ao uso que fazem da informação dada pelos utilizadores	**,442*****	**,420*****	**,464*****	1	
	,000	,000	,000		
	219	219	219	219	
Dispor de mecanismos ativos para mitigar o roubo de identidade	**,363*****	**,405*****	**,484*****	**,537*****	1
	,000	,000	,000	,000	
	219	219	219	219	219
*** p < 0,001; ** p < 0,01; * p < 0,05					

Componente 2 - Segurança da informação arquivada na rede social

	A rede social ter (por defeito) as funcionalidades que usam a localização desligadas ou desativadas	Ter a garantia de que pessoas não autorizadas não tenham acesso às minhas informações pessoais	Ter a garantia de que a informação fornecida à rede social não pode ser alterada por terceiros	Saber que toda a informação fornecida à rede social está segura (de outros utilizadores ou agentes exteriores)	Saber que a minha informação só pode ser acedida por mim (por exemplo, usando mecanismos de encriptação)
A rede social ter (por defeito) as funcionalidades que usam a localização desligadas ou desativadas	1				
	219				
Ter a garantia de que pessoas não autorizadas não tenham acesso às minhas informações pessoais	**,309*****	1			
	,000				
	219	219			
Ter a garantia de que a informação fornecida à rede social não pode ser alterada por terceiros	**,219****	**,592*****	1		
	,001	,000			
	219	219	219		
Saber que toda a informação fornecida à rede social está segura (de outros utilizadores ou agentes exteriores)	**,247*****	**,635*****	**,526*****	1	
	,000	,000	,000		
	219	219	219	219	
Saber que a minha informação só pode ser acedida por mim (por exemplo, usando mecanismos de encriptação)	**,304*****	**,397*****	**,406*****	**,498*****	1
	,000	,000	,000	,000	
	219	219	219	219	219
*** p < 0,001; ** p < 0,01; * p < 0,05					

Componente 3 - Mecanismos de proteção reforçados na rede social

	A rede social deve oferecer mecanismos de autenticação reforçados (por exemplo: autenticação a 2 fatores (password + código), autenticação com certificados pessoais, obrigatoriedade de usar passwords muito complexas, etc.)	A rede social garantir um elevado nível de segurança	A rede social possibilitar um elevado nível de privacidade	Ao usar uma rede social ter o cuidado de não revelar informação pessoal ou confidencial
A rede social deve oferecer mecanismos de autenticação reforçados (por exemplo: autenticação a 2 fatores (password + código), autenticação com certificados pessoais, obrigatoriedade de usar passwords muito complexas, etc.)	1			
	219			
A rede social garantir um elevado nível de segurança	**,530*****	1		
	,000			
	219	219		
A rede social possibilitar um elevado nível de privacidade	**,317*****	**,552*****	1	
	,000	,000		
	219	219	219	
Ao usar uma rede social ter o cuidado de não revelar informação pessoal ou confidencial	**,384*****	**,528*****	**,426*****	1
	,000	,000	,000	
	219	219	219	219
*** p < 0,001; ** p < 0,01; * p < 0,05				

Correlação entre as 3 dimensões obtidas

	Conhecimento de quem pode aceder à informação privada	Segurança da informação arquivada na rede social	Mecanismos de proteção reforçados na rede social
Conhecimento de quem pode aceder à informação privada	1		
	219		
Segurança da informação arquivada na rede social	**,631*****	1	
	,000		
	219	219	
Mecanismos de proteção reforçados na rede social	**,583*****	**,573*****	1
	,000	,000	
	219	219	219

*** p < 0,001; ** p < 0,01; * p < 0,05

Tabela de frequências de índices relativos às dimensões obtidas no objetivo 2

Conhecimento de quem pode aceder à informação privada		
	N	**%**
2,60	1	,5
2,80	1	,5
3,20	2	,9
3,40	4	1,8
3,60	3	1,4
3,80	6	2,7
4,00	20	9,1
4,20	20	9,1
4,40	17	7,8
4,60	29	13,2
4,80	27	12,3
5,00	89	40,6
Total	219	100,0

Segurança da informação arquivada na rede social		
	N	**%**
2,80	1	,5
3,00	1	,5
3,40	2	,9
3,60	3	1,4
3,80	4	1,8
4,00	20	9,1
4,20	9	4,1
4,40	17	7,8
4,60	39	17,8
4,80	40	18,3
5,00	83	37,9
Total	219	100,0

Mecanismos de proteção reforçados na rede social		
	N	**%**
3,00	4	1,8
3,25	3	1,4
3,50	6	2,7
3,75	12	5,5
4,00	18	8,2
4,25	30	13,7
4,50	28	12,8
4,75	45	20,5
5,00	73	33,3
Total	219	100,0

Objetivo 4 - Análise de Componentes Principais – Questão 4 (Parte II)

KMO e Teste de Bartlett		
KMO		,861
Teste de Bartlett	Chi-Quadrado aprox.	1871,691
	Graus de liberdade	276
	Sig.	,000

Variância total explicada						
Componentes	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**
1	7,152	29,801	29,801	3,193	13,303	13,303
2	2,006	8,358	38,159	2,569	10,703	24,005
3	1,692	7,049	45,208	2,279	9,495	33,500
4	1,275	5,311	50,519	2,248	9,366	42,866
5	1,153	4,805	55,324	2,109	8,789	51,655
6	1,087	4,530	59,855	1,968	8,200	59,855
7	,965	4,020	63,875			
8	,888	3,702	67,577			
9	,818	3,410	70,987			
10	,799	3,331	74,317			
11	,693	2,886	77,203			
12	,651	2,712	79,916			
13	,590	2,458	82,373			
14	,578	2,409	84,782			
15	,514	2,143	86,925			
16	,482	2,006	88,931			
17	,438	1,824	90,755			
18	,402	1,676	92,432			
19	,378	1,574	94,005			
20	,358	1,492	95,497			
21	,326	1,360	96,857			
22	,286	1,193	98,050			
23	,259	1,079	99,129			
24	,209	,871	100,000			

Método de Extração: Análise de componentes principais

Matriz de Componentes						
Componentes	1	2	3	4	5	6
1	,528	,476	,338	,383	,353	,329
2	,532	-,198	,387	-,525	-,477	,159
3	-,423	,248	,763	,080	-,169	-,377
4	-,479	,300	-,008	-,176	-,213	,777
5	-,169	-,494	,355	-,284	,689	,214
6	-,032	-,582	,165	,677	-,316	,273

Método de Extração: Análise de componentes principais.

Método de rotação: Varimax e normalização de Kaiser.

Correlações

Componente 1 - Partilha de conteúdos de terceiros

	Partilhar links, notícias e blogs	Partilhar música e filmes	Partilhar conteúdos cómicos	Partilhar pensamentos e sentimentos	Sugerir amigos
Partilhar links, notícias e blogs	1				
	213				
Partilhar música e filmes	**,620*****	1			
	,000				
	213	213			
Partilhar conteúdos cómicos	**,699*****	**,548*****	1		
	,000	,000			
	213	213	213		
Partilhar pensamentos e sentimentos	**,452*****	**,565*****	**,441*****	1	
	,000	,000	,000		
	213	213	213	213	
Sugerir amigos	**,387*****	**,378*****	**,364*****	**,292*****	1
	,000	,000	,000	,000	
	213	213	213	213	213
*** p < 0,001; ** p < 0,01; * p < 0,05					

Componente 2 - Participar nas redes sociais

	Aceitar e fazer pedidos de amizade	Comentar "posts" e mensagens de outras pessoas	Fazer Gostos/Likes/ Love, etc. ...	Identificar amigos
Aceitar e fazer pedidos de amizade	1			
	213			
Comentar "posts" e mensagens de outras pessoas	**,451*****	1		
	,000			
	213	213		
Fazer Gostos/Likes/Love, etc. ...	**,374*****	**,549*****	1	
	,000	,000		
	213	213	213	
Identificar amigos	**,487*****	**,526*****	**,454*****	1
	,000	,000	,000	
	213	213	213	213
*** p < 0,001; ** p < 0,01; * p < 0,05				

Componente 3 - Integração em grupos e comunidades

	Criar e dinamizar grupos de interesse ou comunidades	Fazer parte de grupos de interesse ou comunidades	Fazer inquéritos e sondagens	Criar e agendar eventos
Criar e dinamizar grupos de interesse ou comunidades	1			
	213			
Fazer parte de grupos de interesse ou comunidades	**,369*****	1		
	,000			
	213	213		
Fazer inquéritos e sondagens	**,379*****	**,360*****	1	
	,000	,000		
	213	213	213	
Criar e agendar eventos	**,546*****	**,300*****	**,341*****	1
	,000	,000	,000	
	213	213	213	213
*** p < 0,001; ** p < 0,01; * p < 0,05				

Componente 4 - Conversar e manter contacto com amigos

	Manter contacto com amigos e familiares distantes	Ouvir música e vídeos	Manter contacto com antigos amigos	Conversas através de mensagens instantâneas (Chat)
Manter contacto com amigos e familiares distantes	1			
	213			
Ouvir música e vídeos	**,323*****	1		
	,000			
	213	213		
Manter contacto com antigos amigos	**,650*****	**,256*****	1	
	,000	,000		
	213	213	213	
Conversas através de mensagens instantâneas (Chat)	**,331*****	**,354*****	**,292*****	1
	,000	,000	,000	
	213	213	213	213
*** p < 0,001; ** p < 0,01; * p < 0,05				

Componente 5 - Noticias, Atualidades e contacto com marcas e empresas

	Ver notícias e atualidades	Seguir informação sobre produtos, serviços e empresas	Seguir personalidades públicas ou ídolos
Ver notícias e atualidades	1		
	213		
Seguir informação sobre produtos, serviços e empresas	**,488*****	1	
	,000		
	213	213	
Seguir personalidades públicas ou ídolos	**,453*****	**,440*****	1
	,000	,000	
	213	213	213
*** p < 0,001; ** p < 0,01; * p < 0,05			

Componente 6 - Jogos online, concursos e aplicações usadas nas redes sociais

	Jogar jogos on-line	Partilhar a minha localização	Participar em concursos, sorteios e inquéritos	Usar aplicações oferecidas dentro da rede social
Jogar jogos on-line	1			
	213			
Partilhar a minha localização	**,275*****	1		
	,000			
	213	213		
Participar em concursos, sorteios e inquéritos	**,253*****	**,285*****	1	
	,000	,000		
	213	213	213	
Usar aplicações oferecidas dentro da rede social	**,380*****	**,297*****	**,284*****	1
	,000	,000	,000	
	213	213	213	213
*** p < 0,001; ** p < 0,01; * p < 0,05				

Correlação entre as 6 dimensões obtidas

	Partilha de conteúdos de terceiros	Participar nas redes sociais	Integração em grupos e comunidades	Conversar e manter contacto com amigos	Noticias, Atualidades e contacto com marcas e empresas	Jogos online, concursos e aplicações usadas nas redes sociais
Partilha de conteúdos de terceiros	1					
	213					
Participar nas redes sociais	**,513*****	1				
	,000					
	213	213				

	Partilha de conteúdos de terceiros	Participar nas redes sociais	Integração em grupos e comunidades	Conversar e manter contacto com amigos	Noticias, Atualidades e contacto com marcas e empresas	Jogos online, concursos e aplicações usadas nas redes sociais
Integração em grupos e comunidades	**,408*****	**,480*****	1			
	,000	,000				
	213	213	213			
Conversar e manter contacto com amigos	**,359*****	**,539*****	**,338*****	1		
	,000	,000	,000			
	213	213	213	213		
Noticias, Atualidades e contacto com marcas e empresas	**,362*****	**,490*****	**,240*****	**,511*****	1	
	,000	,000	,000	,000		
	213	213	213	213	213	
Jogos online, concursos e aplicações usadas nas redes sociais	**,494*****	**,484*****	**,335*****	**,351*****	**,460*****	1
	,000	,000	,000	,000	,000	
	213	213	213	213	213	213
*** p < 0,001; ** p < 0,01; * p < 0,05						

Tabela de frequências de índices relativos às dimensões obtidas no objetivo 4

Partilha de conteúdos de terceiros		
	N	**%**
1,00	25	11,7
1,20	13	6,1
1,40	14	6,6
1,60	16	7,5
1,80	17	8,0
2,00	15	7,0
2,20	20	9,4
2,40	28	13,1
2,60	16	7,5
2,80	14	6,6
3,00	11	5,2
3,20	1	,5
3,40	5	2,3
3,60	9	4,2
3,80	4	1,9
4,00	1	,5
4,20	1	,5
4,60	1	,5

Participar nas redes sociais		
	N	**%**
1,00	1	,5
1,50	2	,9
1,75	8	3,8
2,00	8	3,8
2,25	11	5,2
2,50	10	4,7
2,75	26	12,2
3,00	28	13,1
3,25	25	11,7
3,50	26	12,2
3,75	19	8,9
4,00	23	10,8
4,25	8	3,8
4,50	11	5,2
4,75	5	2,3
5,00	2	,9
Total	213	100,0

4,80	2	,9
Total	213	100,0

Integração em grupos e comunidades		
	N	**%**
1,00	7	3,3
1,25	4	1,9
1,50	17	8,0
1,75	9	4,2
2,00	19	8,9
2,25	24	11,3
2,50	28	13,1
2,75	23	10,8
3,00	20	9,4
3,25	25	11,7
3,50	18	8,5
3,75	5	2,3
4,00	6	2,8
4,25	5	2,3
4,50	2	,9
4,75	1	,5
	213	100,0

Conversar e manter contacto com amigos		
	N	**%**
1,00	1	,5
1,50	1	,5
2,00	4	1,9
2,25	3	1,4
2,50	6	2,8
2,75	8	3,8
3,00	19	8,9
3,25	10	4,7
3,50	19	8,9
3,75	31	14,6
4,00	27	12,7
4,25	30	14,1
4,50	23	10,8
4,75	12	5,6
5,00	19	8,9
	213	100,0

Noticias, Atualidades e contacto com marcas e empresas		
	N	**%**
1,00	1	,5
1,33	9	4,2
1,67	11	5,2
2,00	12	5,6
2,33	17	8,0
2,67	23	10,8
3,00	37	17,4
3,33	27	12,7
3,67	27	12,7
4,00	24	11,3
4,33	14	6,6
4,67	6	2,8
5,00	5	2,3
Total	213	100,0

Jogos online, concursos e aplicações usadas nas redes sociais		
	N	**%**
1,00	29	13,6
1,25	20	9,4
1,50	28	13,1
1,75	26	12,2
2,00	30	14,1
2,25	29	13,6
2,50	14	6,6
2,75	15	7,0
3,00	10	4,7
3,25	6	2,8
3,50	3	1,4
3,75	1	,5
4,00	2	,9
Total	213	100,0

Objetivo 5 - Análise de Componentes Principais – Questão 6 (Parte II)

KMO e Teste de Bartlett		
KMO		,890
Teste de Bartlett	Chi-Quadrado aprox.	1687,705
	Graus de liberdade	136
	Sig.	,000

Variância total explicada

Componentes	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**
1	6,665	39,204	39,204	4,334	25,493	25,493
2	2,220	13,058	52,262	3,598	21,164	46,658
3	1,530	9,002	61,264	2,483	14,606	61,264
4	,882	5,187	66,451			
5	,773	4,545	70,995			
6	,704	4,141	75,137			
7	,588	3,460	78,597			
8	,551	3,241	81,838			
9	,522	3,068	84,906			
10	,422	2,483	87,389			
11	,409	2,407	89,796			
12	,396	2,332	92,128			
13	,361	2,123	94,251			
14	,279	1,643	95,894			
15	,268	1,577	97,471			
16	,234	1,376	98,847			
17	,196	1,153	100,000			

Método de Extração: Análise de componentes principais

Matriz de Componentes

Componentes	1	2	3
1	,690	,592	,415
2	-,720	,620	,311
3	-,073	-,514	,855

Método de Extração: Análise de componentes principais.
Método de rotação: Varimax e normalização de Kaiser.

Correlações

Componente 1 – Cultivar relacionamentos e partilhar informação

	Divulgar dados pessoais online satisfaz as minhas necessidades sociais (de alguma forma)	Divulgar dados pessoais online ajuda-me a cultivar bons relacionamentos	Ter um perfil muito detalhado nas redes sociais	Partilhar coisas sobre mim com contactos casuais	Partilhar o meu dia-a-dia	Tenho orgulho em dizer às pessoas que estou nas redes sociais
Divulgar dados pessoais online satisfaz as minhas necessidades sociais (de alguma forma)	1					
	200					
Divulgar dados pessoais online ajuda-me a cultivar bons relacionamentos	**,765*****	1				
	,000					
	200	200				
Ter um perfil muito detalhado nas redes sociais	**,603*****	**,546*****	1			
	,000	,000				
	200	200	200			
Partilhar coisas sobre mim com contactos casuais	**,626*****	**,618*****	**,550*****	1		
	,000	,000	,000			
	200	200	200	200		
Partilhar o meu dia-a-dia	**,593*****	**,568*****	**,560*****	**,561*****	1	
	,000	,000	,000	,000		
	200	200	200	200	200	
Tenho orgulho em dizer às pessoas que estou nas redes sociais	**,527*****	**,408*****	**,606*****	**,487*****	**,516*****	1
	,000	,000	,000	,000	,000	
	200	200	200	200	200	200
*** p < 0,001; ** p < 0,01; * p < 0,05						

Componente 2 – Diversão, rotina e recolha de informação

	Relaxar e descomprimir nas redes sociais	Diversão ao passar tempo nas redes sociais	As redes sociais online fazem parte da minha rotina diária	Reunir rapidamente e em tempo real informação ou notícias atualizada/s sobre a minha cidade, país ou mundo	Aproveitar ao máximo todos os momentos livres para verificar o estado nas redes sociais (na casa de banho, transportes públicos, filas de espera, etc...)	Sinto que faço parte da comunidade da rede social que mais uso	Agiliza o contacto com colegas e professores
Relaxar e descomprimir nas redes sociais	1						
	200						
Diversão ao passar tempo nas redes sociais	**,694*****	1					
	,000						
	200	200					
As redes sociais online fazem parte da minha rotina diária	**,539*****	**,580****	1				
	,000	,000					
	200	200	200				
Reunir rapidamente e em tempo real informação ou notícias atualizada/s sobre a minha cidade, país ou mundo	**,483*****	**,420*****	**,367*****	1			
	,000	,000	,000				
	200	200	200	200			
Aproveitar ao máximo todos os momentos livres para verificar o estado nas redes sociais (na casa de banho, transportes públicos, filas de espera, etc...)	**,549*****	**,506*****	**,638*****	**,326*****	1		
	,000	,000	,000	,000			
	200	200	200	200	200		
Sinto que faço parte da comunidade da rede social que mais uso	**,543*****	**,481*****	**,557*****	**,298*****	**,533*****	1	
	,000	,000	,000	,000	,000		
	200	200	200	200	200	200	

	Relaxar e descomprimir nas redes sociais	Diversão ao passar tempo nas redes sociais	As redes sociais online fazem parte da minha rotina diária	Reunir rapidamente e em tempo real informação ou notícias atualizada/s sobre a minha cidade, país ou mundo	Aproveitar ao máximo todos os momentos livres para verificar o estado nas redes sociais (na casa de banho, transportes públicos, filas de espera, etc...)	Sinto que faço parte da comunidade da rede social que mais uso	Agiliza o contacto com colegas e professores
Agiliza o contacto com colegas e professores	**,329*****	**,328*****	**,416*****	**,360*****	**,287*****	**,294*****	1
	,000	,000	,000	,000	,000	,000	
	200	200	200	200	200	200	200
*** p < 0,001; ** p < 0,01; * p < 0,05							

Componente 3 – Rede profissional, *networking* e grupos de trabalho

	Construir e manter uma rede de contactos profissionais	Construir um perfil público com vista a maximizar a exposição e o networking	Partilhar conteúdos relevantes para a minha atividade profissional	Organizar grupos de trabalho para atividades de estudo
Construir e manter uma rede de contactos profissionais	1			
	200			
Construir um perfil público com vista a maximizar a exposição e o networking	**,626*****	1		
	,000			
	200	200		
Partilhar conteúdos relevantes para a minha atividade profissional	**,500*****	**,490*****	1	
	,000	,000		
	200	200	200	
Organizar grupos de trabalho para atividades de estudo	**,342*****	**,273*****	**,339*****	1
	,000	,000	,000	
	200	200	200	200
*** p < 0,001; ** p < 0,01; * p < 0,05				

Correlação entre as 3 dimensões obtidas

	Cultivar relacionamentos e partilhar informação	Diversão, rotina e recolha de informação	Rede profissional, networking e grupos de trabalho
Cultivar relacionamentos e partilhar informação	1		
	200		
Diversão, rotina e recolha de informação	**,490*****	1	
	,000		
	200	200	
Rede profissional, networking e grupos de trabalho	**,454*****	**,509*****	1
	,000	,000	
	200	200	200
*** p < 0,001; ** p < 0,01; * p < 0,05			

Tabela de frequências de índices relativos às dimensões obtidas no objetivo 5

Cultivar relacionamentos e partilhar informação		
	N	**%**
1,00	43	21,5
1,17	25	12,5
1,33	21	10,5
1,50	20	10,0
1,67	19	9,5
1,83	13	6,5
2,00	16	8,0
2,17	7	3,5
2,33	6	3,0
2,50	6	3,0
2,67	6	3,0
2,83	5	2,5
3,00	5	2,5
3,17	1	,5
3,33	2	1,0
3,67	1	,5
4,00	1	,5
4,33	1	,5
4,67	1	,5
5,00	1	,5
Total	200	100,0

Lazer, rotina e recolha de informação		
	N	**%**
1,00	2	1,0
1,14	2	1,0
1,57	1	,5
1,71	4	2,0
2,00	6	3,0
2,14	3	1,5
2,29	9	4,5
2,43	13	6,5
2,57	15	7,5
2,71	16	8,0
2,86	11	5,5
3,00	16	8,0
3,14	14	7,0
3,29	8	4,0
3,43	19	9,5
3,57	13	6,5
3,71	9	4,5
3,86	8	4,0
4,00	4	2,0
4,14	7	3,5
4,29	6	3,0
4,43	4	2,0
4,71	4	2,0
4,86	2	1,0
5,00	4	2,0
Total	200	100,0

Rede profissional, networking e grupos de trabalho		
	N	**%**
1,00	2	1,0
1,50	5	2,5
1,75	6	3,0
2,00	18	9,0
2,25	13	6,5
2,50	14	7,0
2,75	25	12,5
3,00	23	11,5
3,25	20	10,0

	N	%
3,50	16	8,0
3,75	14	7,0
4,00	23	11,5
4,25	4	2,0
4,50	9	4,5
4,75	6	3,0
5,00	2	1,0
Total	200	100,0